CONTRIBUTIONS TO THE THEORY OF THE DIOPHANTINE EQUATION

$$Ax^n - By^n = C$$

BY

ADOLF AF EKENSTAM

Almqvist & Wiksells Boktryckeri AB

UPPSALA 1959

CONTRIBUTIONS TO THE THEORY OF THE DIOPHANTINE EQUATION

$$Ax^n - By^n = C$$

Inaugural Dissertation

BY

ADOLF AF EKENSTAM

FIL. LIC., V–D.

BY DUE PERMISSION OF
THE FACULTY OF SCIENCE OF THE UNIVERSITY
OF UPPSALA, TO BE PUBLICLY DISCUSSED
IN THE LECTURE HALL OF THE INSTITUTE
OF MATHEMATICS,
ON DECEMBER 5, 1959, AT 10 A.M.,
FOR THE DEGREE OF DOCTOR
OF PHILOSOPHY

Almqvist & Wiksells Boktryckeri AB

UPPSALA 1959

CONTRIBUTIONS TO THE THEORY OF THE DIOPHANTINE EQUATION

$$Ax^n - By^n = C$$

BY

ADOLF AF EKENSTAM

R. UNIV.
BIBLIOTHEEK
LEIDEN

Almqvist & Wiksells Boktryckeri AB

UPPSALA 1959

In publishing this dissertation it is a particular pleasure for me to thank my teacher, Professor Trygve Nagell, who has followed my work with interest and to whom I am indebted for many good advice.

I should also like to thank Fil. lic. Lars Fjellstedt for the many things I learnt from him and for the great interest he has always shown for my work.

Discussions with some of my colleagues at the Mathematical Institute have also meant a great deal for my work and I would like to take this opportunity of acknowledging my indebtedness to them.

My thanks are further due to Miss Margareta Dahlborn who has revised the English text.

Uppsala, September 1959.

Adolf af Ekenstam.

1. According to a theorem by Thue [20]* the Diophantine equation

$$f_n(x, y) = C$$

where $f_n(x, y)$ is a binary irreducible form of degree $n \geqslant 3$ with coefficients which are rational integers and C is a constant, has only a finite number of solutions in rational integers x, y.

To obtain more clearly defined results, it is necessary to specialize the form $f_n(x, y)$. A series of investigations from different points of view have been made on the Diophantine equation

$$A x^n - B y^n = C \tag{1.1}$$

where A, B, C are given integers. Thue [21] treated (1.1) in some cases with certain conditions on the integers A, B, C. The results of Thue are included in the following proposition proved by Siegel [15].

Theorem I: Let A, B and C be positive integers, $n \geqslant 3$. If

$$(A B)^{\frac{n}{2}-1} \geqslant C^{2n-2} 4 \left[n \prod_{p/n} p^{\frac{1}{p-1}} \right]^n$$

where p runs through all the different primes dividing n, then the inequality

$$|A x^n - B y^n| \leqslant C \tag{1.2}$$

has at most one solution in natural relatively prime numbers x and y.

Siegel obtains the result with the aid of theorems from the theory of hypergeometrical functions. By sharpening suitable inequalities in Siegel's proof when $C = 1$, Domar [2] has deduced the following two supplementary theorems:

Theorem II a: The Diophantine equation

$$|A x^n - B y^n| = 1$$

where A and B are positive integers and $n \geqslant 5$ has at most two solutions in natural numbers x and y.

* Figures in [ ] refer to the Bibliography at the end of this paper.

Theorem II b: The Diophantine equation

$$|x^n - My^n| = 1$$

where M is a natural number and $n \geqslant 5$ has at most one solution in positive integers x, y except possibly for $M = 2$ and if $n = 5$ or 6 for $M = 2^n \pm 1$.

2. Without using the method of Thue and with arguments taken exclusively from the theory of numbers, Delaunay [1], Nagell [13], Ljunggren [7, 8], Tartakowsky [19] and others have treated (1.1) in special cases. We cite the following theorems:

Theorem III: (Nagell [13]). Let the numbers A, B and C satisfy the following conditions: C is one of the numbers 1 or 3; A and B are coprime integers such that $1 \leqslant A < B$; AB is not divisible by 3 when $C = 3$; AB is not divisible by the cube of any prime.

The Diophantine equation

$$Ax^3 + By^3 = C \tag{2.1}$$

has at most one solution in integers x and y with $xy \neq 0$ except the equation $2x^3 + y^3 = 3$, which has exactly two solutions: $x = y = 1$, $x = 4$, $y = -5$.

The Diophantine equation (2.1) is said to belong to the class of the (real) cubic field

$$K\left(\sqrt[3]{\frac{A}{B}}\right).$$

Among all the equations belonging to the same class there is at most one equation which is solvable in integers x and y with $xy \neq 0$ except in the following cases:

In the class of the field $K(\sqrt[3]{2})$ the existing equations are:

$$x^3 + 2y^3 = 1, \quad x^3 + 2y^3 = 3, \quad x^3 + 4y^3 = 3, \quad x^3 + 4y^3 = 1.$$

The first three equations are solvable; the last one is not solvable for $y \neq 0$.

In the class of the field $K(\sqrt[3]{20})$ the existing equations are:

$$x^3 + 20y^3 = 1, \quad 2x^3 + 5y^3 = 3, \quad x^3 + 20y^3 = 3, \quad 2x^3 + 5y^3 = 1,$$
$$x^3 + 50y^3 = 1, \quad 4x^3 + 25y^3 = 1, \quad x^3 + 50y^3 = 3, \quad 4x^3 + 25y^3 = 3.$$

Only the first two equations are solvable; the others are not solvable for $y \neq 0$.

Concerning Theorem III see also Ljunggren [9].

Delaunay [1] and Nagell [13] have both established results on a special case of (1.1) when $A = C = 1$ and $n = 3$. In fact the Diophantine equation

$$x^3 + By^3 = 1$$

has at most one solution in integers x, $y \neq 0$. If $x = x_1$, $y = y_1$ is a solution, $x_1 + y_1 \sqrt[3]{B}$ is the fundamental unit of the field $K(\sqrt[3]{B})$ except for $B = 19$, 20 and 28 when it is the square of the fundamental unit.

Theorem IV: (Ljunggren [7]). The Diophantine equation

$$Ax^4 - By^4 = C \tag{2.2}$$

where A and B are positive integers and $C = 1$, 2, 4 or 8 has at most one solution in positive integers x and y.

Among all the equations (2.2) belonging to the same class of the field $K\left(\sqrt[4]{\frac{A}{B}}\right)$ there is at most one which is solvable in positive integers x and y except one case, the field $K(\sqrt[4]{5})$. The equations

$$x^4 - 5y^4 = 1 \text{ and } x^4 - 5y^4 = -4$$

are both solvable.

Theorem V: (Ljunggren [8]). The Diophantine equation

$$Ax^6 - By^6 = C \tag{2.3}$$

where A and B are positive integers and $C = 1$, 2, 3, 4 or 6 has at most one solution in positive integers x and y.

Among all the equations belonging to the class of the field $K\left(\sqrt[6]{-27\frac{A}{B}}\right)$ there is at most one which is solvable in positive integers x and y.

In the proofs of the theorems III–V the authors give methods to decide if the regarded equation is solvable and to determine all the possible solutions.

Tartakowsky [19] has proved the following theorem (published before Theorem IV):

Theorem VI: Let M be a positive integer $\neq 15$ which is not a perfect square. The Diophantine equation

$$x^4 - My^4 = 1 \tag{2.4}$$

has at most one solution in positive integers x, y and if $x = x_1$, $y = y_1$ is a solution, the number $x_1^2 + y_1^2\sqrt{M}$ is the fundamental unit ε or its square of the field $R(\sqrt{M})$, the latter occurring only in a finite number of cases and only if $N(\varepsilon) = 1$. If $N(\varepsilon) = -1$, (2.4) has no solutions apart from the case $M = 5$.

It is difficult, however, to read Tartakowsky's proof and Ljunggren [7] has later given a proof which is included in Theorem IV above.

According to a hypothesis by Tartakowsky [19] the Diophantine equation

$$x^{2s} - My^{2s} = 1$$

where M is a positive integer that is not a perfect d:th power and d a divisor of $2s$ and where $s \geqslant 3$, has at most one solution in natural numbers x, y. If $x = x_1$, $y = y_1$ is a solution then $x_1^s + y_1^s\sqrt{M}$ is the fundamental unit of $R(\sqrt{M})$ its square or its fourth power, the last two cases can only occur for a finite number of M.

Tartakowsky has not published any proof but he promised one. However, this proof has never appeared.

The method of the authors mentioned above is based on the theory of units in quadratic, cubic or biquadratic fields and further on arguments of divisibility. In the treatises an important fact is that in the fields where the operations were made, the field was either primitive and had only one fundamental unit, or it was imprimitive but had a subfield with only one fundamental unit.

With a method called the p-adic method Skolem [17] has been able to treat different Diophantine equations, among others the equation

$$x^5 + My^5 = 1$$

which has no solutions in integers $\neq 0$ for $M = 4$, 8 and 16 and only the solution $x = -1$, $y = 1$ when $M = 2$. The proof is based on studies of the units of the ring $R(\sqrt[5]{2})$ where a system of fundamental units was known.

Our contributions to the problem concerning the Diophantine equation (1.1) are found in the following three chapters. In the first

chapter we shall show—without using the theory of units in algebraic fields as in Nagell's and Ljunggren's papers—that among all the equations belonging to the same class of the field $K\left(\sqrt[n]{\frac{A}{B}}\right)$ at most one is solvable if the coefficients A, B, C satisfy certain conditions. In Chapter II we shall determine an upper limit to the number of integral solutions in integers x, y belonging to a given imaginary field. The proof is established for $n=3$ and the field $K(\sqrt{-3})$ and for $n=4$ and the field $K(\sqrt{-1})$. We here use and generalize arguments from Siegel's work and from the theory of the quadratic fields $K(\sqrt{-1})$ and $K(\sqrt{-3})$.

At last in Chapter III we shall give a proof of Tartakowsky's hypothesis and that in a somewhat extended form by using an idea from the first chapter about the solvability of Diophantine equations belonging to the same class of the field $K\left(\sqrt[n]{\frac{A}{B}}\right)$.

ON DIOPHANTINE EQUATIONS BELONGING TO THE SAME CLASS

§ 1. Definitions and theorems

3. Let A_1, A_2, B_1, B_2, C_1 and C_2 be positive integers. If the fields $K\left(\sqrt[n]{\frac{A_1}{B_1}}\right)$ and $K\left(\sqrt[n]{\frac{A_2}{B_2}}\right)$ are identical, the Diophantine equations

$$|A_1 x^n - B_1 y^n| = C_1$$
$$|A_2 x^n - B_2 y^n| = C_2$$

are said to belong to the same class of the field $K\left(\sqrt[n]{\frac{A_1}{B_1}}\right)$ or shorter to the same class.

We shall establish the following three theorems:

Theorem A: Let A_ν, B_ν and C_ν be positive integers such that $(A_\nu \cdot B_\nu, C_\nu) = 1$ and $A_\nu \cdot B_\nu$ is not divisible by the n:th power of a prime. Consider the Diophantine equations

$$|A_\nu x^n - B_\nu y^n| = C_\nu \quad (\nu = 1, 2, \ldots) \tag{3.1}$$

with $n \geqslant 4$ which belong to the same class and put $A_\nu \cdot B_\nu = T_\nu$. Introduce $\min\limits_{\nu=1,2,\ldots} T_\nu = T$ and $\max\limits_{\nu=1,2,\ldots} C_\nu = C$. Suppose that

$$\begin{aligned} T^{\frac{n-5}{4}} &\geqslant C^f n^{n+2} && n \geqslant 6 \\ T^{1/3} &\geqslant C^6 \cdot 12000 && n = 5 \\ T^{1/3} &\geqslant C^6 \cdot 16384 && n = 4 \end{aligned} \tag{3.2}$$

where $f = n$ if $6 \leqslant n \leqslant 13$ and $f = \frac{4}{3}(n-3)$ if $n \geqslant 14$. Under these conditions at most one of the equations (3.1) is solvable in positive relatively prime integers x and y.

Theorem B: Among all the equations

$$|A_\nu x^n - B_\nu y^n| = 1 \quad (\nu = 1, 2, \ldots) \tag{3.3}$$

with $n \geqslant 5$ belonging to the same class, at most two are solvable in positive integers x and y. — If $n \geqslant 8$ and none of the equations has the solution $x = y = 1$, then at most one of the equations is solvable with $x, y > 0$. The same case is true even if $5 \leqslant n \leqslant 7$ if none of the equations has the solution $x = y = 1$ or $x = 2, y = 1$ (or $x = 1, y = 2$).

Theorem C: Let $M \geqslant 2$ be a positive integer and $n \geqslant 5$. Consider the $\varphi(n)$* equations

$$|x^n - M^s y^n| = 1 \tag{3.4}$$

where s runs through the numbers $1, \ldots n-1$, so that $(n, s) = 1$ and suppose that the field $K(\sqrt[n]{M})$ is not identical with any of the fields $K(\sqrt[n]{2})$, $K(\sqrt[5]{31})$, $K(\sqrt[5]{33})$, $K(\sqrt[6]{63})$, $K(\sqrt[6]{65})$, $K(\sqrt[7]{127})$, $K(\sqrt[7]{129})$. Then at most one of the equations is solvable in positive integers x and y.

§ 2. Some lemmata

4. Let A_ν, B_ν and C_ν be positive integers satisfying the following conditions: $(A_\nu \cdot B_\nu, C_\nu) = 1$, $A_\nu \cdot B_\nu$ is not divisible by the n:th power of a prime. Consider the Diophantine equations

$$|A_\nu x^n - B_\nu y^n| = C_\nu \quad (\nu = 1, 2, \ldots) \tag{4.1}$$

with $n \geqslant 4$ which belong to the same class. Introduce $\min\limits_{\nu=1,2,\ldots} A_\nu \cdot B_\nu = T$, $\max\limits_{\nu=1,2,\ldots} C_\nu = C$ and suppose that

$$\begin{aligned} T^{\frac{n-5}{4}} &\geqslant C^f \cdot n^{n+2} && n \geqslant 6 \\ T^{1/2} &\geqslant C^6 \cdot 12000 && n = 5 \\ T^{1/2} &\geqslant C^6 \cdot 16384 && n = 4 \end{aligned} \tag{4.2}$$

where $f = n$ if $6 \leqslant n \leqslant 13$ and $f = \frac{4}{3}(n-3)$ if $n \geqslant 14$.

The following lemmata are used in the following reasonings:

Lemma 1: If A, B, C are positive integers satisfying the conditions for A_ν, B_ν and C_ν above, and the number

* When n is a natural number we denote by $\varphi(n)$ the number of natural numbers $\leqslant n$ which are prime to n.

$$\sqrt[n]{\frac{A}{B}}$$

is an algebraic number of degree $< n$, then the Diophantine equation

$$|A x^n - B y^n| = C \tag{4.3}$$

has no solutions in positive integers x and y.

Proof: Since $(A, B) = 1$ we must have $A = a^\alpha$, $B = b^\beta$ with a, b natural numbers and $(\alpha, \beta, n) = f > 1$. Putting $\alpha = \alpha_1 f$, $\beta = \beta_1 f$, $n = n_1 f$ in the equation above we obtain

$$|(a^{\alpha_1} x^{n_1})^f - (b^{\beta_1} y^{n_1})^f| = C.$$

Let us first suppose that f is even. The left-hand member is reducible and it follows

$$C \geqslant (a^{\alpha_1} x^{n_1})^{\frac{f}{2}} + (b^{\beta_1} y^{n_1})^{\frac{f}{2}} \geqslant 2\, T^{1/4}$$

or simpler

$$C^4 \geqslant 2^4 \cdot T$$

which is a contradiction according to (4.2). Suppose next that f is odd. Then it is easily seen that we must have

$$C \geqslant (a^{\alpha_1} x^{n_1})^{f-1} + (b^{\beta_1} y^{n_1})^{f-1} > 2\, T^{1/3}$$

which is impossible. Thus our Lemma is proved.

Remark 1: It is easily seen that for $C = 1$ the lemma is valid without supposing the condition (4.2).

Remark 2: The number of equations belonging to the same class depends both on the value of n and the number of primes of A and B. Suppose for instance that $n = 5$. The equations which belong to the same class as

$$|4 x^5 - 3 y^5| = 1$$

are the following equations (if we do not take into consideration the constant of the right-hand member and put it $= 1$).

$$|24 x^5 - y^5| = 1,\ |324 x^5 - y^5| = 1,\ |18 x^5 - y^5| = 1,\ |432 x^5 - y^5| = 1,$$
$$|16 x^5 - 9 y^5| = 1,\ |81 x^5 - 8 y^5| = 1,\ |27 x^5 - 2 y^5| = 1,$$

in total eight equations belonging to the class of the field $K(\sqrt[5]{\frac{4}{3}})$.

Remark 3: It is clear that the Diophantine equation

$$|A x^n - B y^n| = C$$

has the solution $x = -x_1$, $y = -y_1$ if it has the solution $x = x_1$, $y = y_1$. Therefore it sufficies to consider solutions in positive integers x, y.

5. **Lemma 2:** Consider all the Diophantine equations belonging to the class $K\left(\sqrt[n]{\frac{A_1}{B_1}}\right)$ and choose two arbitrary equations

$$\begin{aligned} |A_i x^n - B_i y^n| &= C_i \\ |A_j x^n - B_j y^n| &= C_j. \end{aligned} \tag{5.1}$$

There is a uniquely determined positive integer k, $(k, n) = 1$, $1 \leqslant k < n$ such that

$$\sqrt[n]{\frac{A_j}{B_j}} = \frac{p}{q} \sqrt[n]{\left(\frac{A_i}{B_i}\right)^k} \tag{5.2}$$

where p, q are positive integers which are relatively prime.

Proof: Since the fields $K\left(\sqrt[n]{\frac{A_i}{B_i}}\right)$, $K\left(\sqrt[n]{\frac{A_j}{B_j}}\right)$ are identical with the field $K\left(\sqrt[n]{\frac{A_1}{B_1}}\right)$ the relations

$$\begin{aligned} \sqrt[n]{\frac{A_i}{B_i}} &= \frac{p_i}{q_i} \sqrt[n]{\left(\frac{A_1}{B_1}\right)^{l_i}} \\ \sqrt[n]{\frac{A_j}{B_j}} &= \frac{p_j}{q_j} \sqrt[n]{\left(\frac{A_1}{B_1}\right)^{l_j}} \end{aligned} \tag{5.3}$$

must hold. The numbers p_i, q_i, p_j, q_j, l_i and l_j are natural numbers and $(p_i, q_i) = (p_j, q_j) = (n, l_i) = (n, l_j) = 1$, $1 \leqslant l_i < n$, $1 \leqslant l_j < n$.
Choose two positive integers k_i and k_j satisfying the conditions

$$\begin{aligned} l_i k_i &\equiv 1 \pmod{n} \\ l_j k_j &\equiv 1 \pmod{n} \end{aligned}$$

which is possible as n and l_i, l_j are relatively prime. We further decide that $1 \leqslant k_i < n$, $1 \leqslant k_j < n$.

(*Remark:* If $(a, n) = 1$, then the linear congruence

$$a x + b \equiv 0 \pmod{n}$$

has exactly one solution modulo n. See e.g. [11].)

From (5.3) it now follows

$$\sqrt[n]{\left(\frac{A_i}{B_i}\right)^{k_i}} = \left(\frac{p_i}{q_i}\right)^{k_i} \sqrt[n]{\left(\frac{A_1}{B_1}\right)^{k_i l_i}} = \frac{p_i'}{q_i'} \sqrt[n]{\frac{A_1}{B_1}}$$

and

$$\sqrt[n]{\left(\frac{A_j}{B_j}\right)^{k_j}} = \left(\frac{p_j}{q_j}\right)^{k_j} \sqrt[n]{\left(\frac{A_1}{B_1}\right)^{k_j l_j}} = \frac{p_i''}{q_i''} \sqrt[n]{\frac{A_1}{B_1}}$$

and consequently

$$\sqrt[n]{\left(\frac{A_i}{B_i}\right)^{k_i}} = \frac{p''}{q''} \sqrt[n]{\left(\frac{A_j}{B_j}\right)^{k_j}}$$

where the numbers p, q with different indices are coprime positive integers.

Since $(k_j, n) = 1$ we can choose a positive integer k_k, $1 \leqslant k_k < n$ such that

$$k_k \cdot k_j \equiv 1 \pmod{n}.$$

Hence

$$\sqrt[n]{\left(\frac{A_i}{B_i}\right)^{k_i k_k}} = \left(\frac{p''}{q''}\right)^{k_k} \sqrt[n]{\left(\frac{A_j}{B_j}\right)^{k_j k_k}} = \frac{p'''}{q'''} \sqrt[n]{\frac{A_j}{B_j}}$$

or

$$\sqrt[n]{\frac{A_j}{B_j}} = \frac{p}{q} \sqrt[n]{\left(\frac{A_i}{B_i}\right)^{k}}$$

where $(p, q) = 1$ and k is the positive integer which satisfies the conditions

$$1 \leqslant k < n \quad k \equiv k_i k_k \pmod{n}.$$

It is evidently $(k, n) = 1$ and Lemma 2 is proved.

6. Suppose that the Diophantine equations

$$|A_i x^n - B_i y^n| = C_i \tag{6.1}$$

$$|A_j x^n - B_j y^n| = C_j \tag{6.2}$$

are solvable with the solutions $x = x_i$, $y = y_i$ resp. $x = x_j$, $y = y_j$ and that they belong to the same class. According to Lemma 2 we have (5.2). Put $L_i = \max(A_i x_i^n, B_i y_i^n)$ e.g. $= A_i x_i^n$ and consequently

$$A_i x_i^n - B_i y_i^n = C_i. \tag{6.3}$$

Suppose further that

$$A_j x_j^n + B_j y_j^n \geqslant A_i x_i^n + B_i y_i^n \tag{6.4}$$

and put $L_j = A_j x_j^n$.

It is now necessary to distinguish between two cases:

$$1°:\ 1 \leqslant k < \frac{n}{2}\,.$$

Lemma 3 a: The following inequalities are true:

$$L_i > T^{1/2} \tag{6.5}$$

$$L_j > \frac{L_i^{n-k}}{[(k+1)\,C]^n}\,. \tag{6.6}$$

Proof: The first inequality immediately follows, for

$$2\,L_i = A_i x_i^n - B_i y_i^n + A_i x_i^n + B_i y_i^n > A_i + B_i \geqslant 2\,T^{1/2}.$$

In order to prove (6.6) we consider

$$\frac{A_i x_i^n - B_i y_i^n}{\sqrt[n]{A_i}\,x_i - \sqrt[n]{B_i}\,y_i} = (A_i x_i^n)^{\frac{n-1}{n}} + \cdots > (A_i x_i^n)^{\frac{n-1}{n}}.$$

According to the definition of C we obtain

$$0 < 1 - \sqrt[n]{\frac{B_i}{A_i}}\,\frac{y_i}{x_i} < \frac{C_i}{L_i} \leqslant \frac{C}{L_i}\,.$$

In the same way we obtain

$$\left| 1 - \sqrt[n]{\frac{B_j}{A_j}}\,\frac{y_j}{x_j} \right| < \frac{C}{L_j}\,. \tag{6.7}$$

Further we have

$$1 - \sqrt[n]{\left(\frac{B_i}{A_i}\right)^k}\left(\frac{y_i}{x_i}\right)^k = \left(1 - \sqrt[n]{\frac{B_i}{A_i}}\,\frac{y_i}{x_i}\right)\left[1 + \sqrt[n]{\frac{B_i}{A_i}}\,\frac{y_i}{x_i} + \cdots + \sqrt[n]{\left(\frac{B_i}{A_i}\right)^{k-1}}\left(\frac{y_i}{x_i}\right)^{k-1}\right]$$

and consequently

$$0 < 1 - \sqrt[n]{\left(\frac{B_i}{A_i}\right)^k}\left(\frac{y_i}{x_i}\right)^k < \frac{k\,C}{L_i}\,. \tag{6.8}$$

From (6.7) and (6.8) it now follows

$$\left| \sqrt[n]{\frac{B_j}{A_j}}\,\frac{y_j}{x_j} - \sqrt[n]{\left(\frac{B_i}{A_i}\right)^k}\left(\frac{y_i}{x_i}\right)^k \right| < \frac{C}{L_j} + \frac{k\,C}{L_i}$$

and according to (5.2)

$$\sqrt[n]{\left(\frac{B_i}{A_i}\right)^k}\left|\frac{q}{p}\,\frac{y_j}{x_j} - \left(\frac{y_i}{x_i}\right)^k\right| < \frac{(k+1)\,C}{\min\,(L_i,\,L_j)}. \tag{6.9}$$

By (5.2) we have

$$q^n A_j B_i^k = p^n A_i^k B_j$$

and since $(p, q) = 1$, p^n divides $A_j B_i^k$, and thus

$$p \leqslant \sqrt[n]{A_j B_i^k}. \tag{6.10}$$

Let us suppose that

$$q\,x_i^k\,y_j = p\,x_j\,y_i^k. \tag{6.11}$$

With regard to (5.2) we obtain

$$A_i^k\,B_j\,x_i^{kn}\,y_j^n = A_j\,B_i^k\,x_j^n\,y_i^{kn}.$$

Since $(A_i, B_i) = (A_j, B_j) = 1$ and from the fact that x_i and y_i resp. x_j and y_j are relatively prime it follows that $B_j y_j^n$ divides $B_i^k\,y_i^{kn}$ and inversely that $B_i^k\,y_i^{kn}$ must divide $B_j y_j^n$. Thus we must have

$$A_i^k\,x_i^{kn} = A_j\,x_j^n$$

$$B_i^k\,y_i^{kn} = B_j\,y_j^n$$

and consequently

$$\left|(A_i x_i^n)^k - (B_i y_i^n)^k\right| = C_j. \tag{6.12}$$

First we consider the case $k = 1$. But from the relations above it follows $A_i x_i^n = A_j x_j^n$, $B_i y_i^n = B_j y_j^n$, which is impossible as the equations (6.1) and (6.2) may be supposed to be different. Suppose next $k \geqslant 2$. From the equation above and (6.3) the contradiction follows:

$$C_j = (A_i x_i^n - B_i y_i^n)\,([A_i x_i^n]^{k-1} + \cdots + [B_i y_i^n]^{k-1}) > T^{1/3} > C.$$

Thus the relation (6.11) cannot hold and instead of (6.11) the inequality

$$\left|q\,x_i^k\,y_j - p\,x_j y_i^k\right| \geqslant 1$$

is true.

Let us return to (6.9). We evidently obtain

$$\sqrt[n]{\left(\frac{B_i}{A_i}\right)^k}\,\frac{1}{p\,x_i^k\,x_j} < \frac{(k+1)\,C}{\min\,(L_i,\,L_j)}\,.$$

and with respect to (6.10) it follows

$$\frac{1}{L_i^{k/n}\,L_j^{1/n}} < \frac{(k+1)\,C}{\min\,(L_i,\,L_j)}$$

If $L_i \leqslant L_j$ we obtain

$$L_j > \frac{L_i^{n-k}}{[(k+1)\,C]^n}$$

and the inequality (6.6) is proved. Suppose that $L_j < L_i$ and it follows

$$[(k+1)\,C]^n\,L_i^k > L_j^{n-1}.$$

But this relation is impossible for with respect to (6.4), (6.5) and (4.2) we obtain

$$\begin{aligned} 0 &\geqslant \tfrac{1}{2}\,(A_i x_i^n + B_i y_i^n - A_j x_j^n - B_j y_j^n) \geqslant A_i x_i^n - A_j x_j^n - C = \\ &= L_i - L_j - C \geqslant L_i - [(k+1)\,C]^{\frac{n}{n-1}}\,L_i^{\frac{k}{n-1}} - C \geqslant \qquad (6.13) \\ &\geqslant L_i^{1/3}\left[T^{1/4} - \left(\frac{n+1}{2}\,C\right)^{\frac{n}{n-1}}\right] - C > C - C = 0. \end{aligned}$$

Thus Lemma 3a is proved.

$$2^{\circ}\colon\ \frac{n}{2} < k < n.$$

Putting $k' = n - k$ where $(k',\ n) = 1$ and $1 \leqslant k' < \frac{n}{2}$ the following lemma is true:

Lemma 3b: The following inequalities are valid

$$L_i > T^{1/2} \qquad (6.14)$$

$$L_j' > \frac{L_i^{n-k'}}{[(k'+1)\,C]^n} \qquad (6.15)$$

where $L_j' = B_j y_j^n$.

The proofs are an analogous to those of Lemma 3a. The relation (6.14) is independent of k and consequently proved. It is easy to see that (5.2) can be written

$$\sqrt[n]{\frac{A_j}{B_j}} = \frac{p'}{q'} \sqrt[n]{\left(\frac{B_i}{A_i}\right)^{k'}} \tag{6.16}$$

where p' and q' are positive integers, $(p', q') = 1$. Further we have

$$0 < 1 - \sqrt[n]{\left(\frac{B_i}{A_i}\right)^{k'}} \left(\frac{y_i}{x_i}\right)^{k'} < \frac{k' C}{L_i} \tag{6.17}$$

and

$$\left| 1 - \sqrt[n]{\frac{A_j}{B_j}} \frac{x_j}{y_j} \right| < \frac{C}{L'_j}. \tag{6.18}$$

From (6.16) it follows that $q' \leqslant \sqrt[n]{B_i^k B_j}$ and if we suppose that

$$p' x_i^{k'} x_j = q' y_i^{k'} y_j$$

it follows

$$A_i^{k'} A_j x_i^{k'n} x_j^n = B_i^{k'} B_j y_i^{k'n} y_j$$

and hence

$$A_i^{k'} x_i^{k'n} = B_j y_j^n$$

$$B_i^{k'} x_i^{k'n} = A_j y_j^n$$

and we obtain

$$\left| (A_i x_i^n)^{k'} - (B_i y_i^n)^{k'} \right| = C_j.$$

But it is evidently clear that this relation is impossible as the corresponding relation (6.12). Consequently the inequality

$$\left| p' x_i^{k'} x_j - q' y_i^{k'} y_j \right| \geqslant 1$$

is true.

According to (6.17) and (6.18) we now obtain

$$\frac{1}{L_i^{k'/n} L_j'^{1/n}} < \frac{(k'+1) C}{\min (L_i, L'_j)}$$

and (6.15) follows analogous to (6.6).

7. Suppose that $1 \leqslant k < \frac{n}{2}$. We need the following lemma:

Lemma 4 a: There exists a unique positive integer m such that

$$s_m L_i^m \leqslant \frac{k}{nC} L_i^{-\frac{k}{n}} L_j^{1-\frac{1}{n}} < s_{m+1} L_i^{m+1} \tag{7.1}$$

where $s_m = \binom{2m}{m} q_m n^m$ and q_m is the product of all the primes of n dividing $m!$; multiple primes being repeated. Further the integer m is $\geqslant 2$ for $n \geqslant 6$ and for $n = 5$, $k = 1$.

If $\frac{n}{2} < k < n$ we put $k' = n - k$ and have

Lemma 4 b: There exists a unique positive integer m' such that

$$s_{m'} L_i^{m'} \leqslant \frac{k'}{nC} L_i^{-\frac{k'}{n}} L_j^{1-\frac{1}{n}} < s_{m'+1} L_i^{m'+1}. \tag{7.2}$$

It is evidently sufficient to prove the first lemma.

Proof: It is easily seen that the numbers $s_t w_i^t$ $(t = 1, 2, \ldots)$ are steadily increasing $\to \infty$ when $t \to \infty$. So it is sufficient to prove that the inequality

$$s_t L_i^t \leqslant \frac{k}{nC} L_i^{-\frac{k}{n}} L_j^{1-\frac{1}{n}} \tag{7.3}$$

is valid for $t = 2$ if $n \geqslant 6$ or $n = 5$, $k = 1$ and for $t = 1$ if $n = 4$ or $n = 5$, $k = 2$. (If $n = 5$ then $k = 1$ or 2).

According to Lemma 3a we obtain if $n \geqslant 6$ or $n = 5$, $k = 1$

$$\frac{k}{s_2 nC} L_i^{-\frac{k}{n}-2} L_j^{1-\frac{1}{n}} > \frac{k L_i^{n-k-3}}{s_2 \cdot n \cdot C\,[(k+1)\,C]^{n-1}}$$

and according to the definition of s_2 and (4.2), (6.5) and since $k < \frac{n}{2}$ it follows for $n \geqslant 6$

$$\frac{k L_i^{n-k-3}}{s_2 nC\,[(k+1)\,C]^{n-1}} \geqslant \frac{T^{\frac{n-5}{4}}}{s_2 nC^n \left(\frac{n+1}{2}\right)^{n-1}} \geqslant \frac{n^{n+2}}{12 n^3 \left(\frac{n+1}{2}\right)^{n-1}} =$$

$$= \frac{2^{n-3}}{3} \cdot \frac{1}{\left(1 + \frac{1}{n}\right)^{n-1}} > 1.$$

With respect to (4.2), (6.5), $n=5$, $k=1$ and $s_2=150$ if $n=5$ we obtain

$$\frac{k L_i^{n-k-3}}{s_2 n C[(k+1)C]^{n-1}} \geqslant \frac{T^{1/2}}{150 \cdot 80 \cdot C^5} \geqslant 1.$$

If $n=4$ and $n=5$, $k=2$ we obtain analogously

$$\frac{k}{s_1 \cdot n \cdot C} L_i^{-\frac{k}{n}-1} L_j^{\frac{n-1}{n}} \geqslant \frac{L_i^{n-2-k}}{s_1 \cdot n \cdot C[(k+1)C]^{n-1}} > \frac{T^{1/2}}{2n^2 C^n (k+1)^{n-1}} > 1.$$

Lemma 5: Let $n \geqslant 6$. If $T^{\frac{n-5}{4}} \geqslant n^{n+2}$, then $T^{\frac{3}{8}(n-3)} > \lambda_n = 4n^n \prod_{p/n} p^{\frac{n}{p-1}}$ where p runs through all the different primes of n.

Proof: We evidently have

$$\lambda_n \leqslant 2^{2+\frac{3n}{4}} \cdot 3^{\frac{n}{4}} \cdot n^{\frac{5n}{4}}$$

and it is seen easily that

$$T^{\frac{3}{8}(n-3)} > n^{\frac{3(n+2)(n-3)}{2(n-5)}} > n^{\frac{3n}{2}+6} > 2^{2+\frac{3n}{4}} \cdot 3^{\frac{n}{4}} \cdot n^{\frac{5n}{4}} \geqslant \lambda_n.$$

§ 3. Hypergeometric functions

8. By means of an approximation to the function $(1-\xi)^{\frac{1}{n}}$ $n>2$ in the interval $0<\xi<1$, Siegel [15] derives suitable inequalities. Changing $\frac{1}{n}$ for $\frac{k}{n}$ where k is a positive integer, $k<\frac{n}{2}$, analogous approximations may be deduced. The number k is the integer mentioned in the former paragraph.

The lemmata $a-d$ in this paragraph are taken from Siegel's paper [15] and are cited without any proofs; the lemmata $e-g$ are proved in an analogous way as the corresponding theorems in the paper just mentioned.

Let ξ be a real number, $0<\xi<1$, and consider the hypergeometric function defined by the series

$$F(\alpha, \beta, \gamma, \xi) = 1 + \frac{\alpha \cdot \beta}{1 \cdot \gamma} \xi + \cdots$$

which consequently satisfies the differential equation

$$\xi(\xi-1)\frac{d^2F}{d\xi^2} + \{(1+\alpha+\beta)\xi - \gamma\}\frac{dF}{d\xi} + \alpha \cdot \beta \cdot F = 0.$$

For every positive integer r the functions

$$A_r(\xi) = F(-\mu - r, -r, -2r, \xi) =$$

$$\sum_{m=0}^{r} \frac{(r+\mu)(r+\mu-1)\ldots(r+\mu-m+1)}{2r(2r-1)\ldots(2r-m+1)} \binom{r}{m} (-\xi)^m \tag{8.1}$$

$$B_r(\xi) = F(\mu - r, -r, -2r, \xi) =$$

$$\sum_{m=0}^{r} \frac{(r-\mu)(r-\mu-1)\ldots(r-\mu-m+1)}{2r(2r-1)\ldots(2r-m+1)} \binom{r}{m} (-\xi)^m \tag{8.2}$$

where μ is a number between 0 and 1, are polynomials of degree r. Introduce the function $C_r(\xi)$ defined by the connection

$$A_r(\xi) - (1-\xi)^{\mu} B_r(\xi) = C_r(\xi). \tag{8.3}$$

Choose μ equal to $\frac{k}{n}$ where k and n are coprime positive integers and $1 \leqslant k < n$. Introduce further

$$s_r = \binom{2r}{r} q_r n^r, \quad u_r = q_r n^r \prod_{m=1}^{r} \left(1 - \frac{k}{m \cdot n}\right) \tag{8.4}$$

where q_r is the product of all the primes of n which divide $r!$; multiple primes being repeated. At last we introduce the functions $G_r(\xi)$ and $H_r(\xi)$ defined by

$$s_r A_r(\xi) = G_r(\xi), \quad s_r B_r(\xi) = H_r(\xi). \tag{8.5}$$

Lemma a: There is a constant $\varrho_r \neq 0$, such that

$$C_r(\xi) = \varrho_r \xi^{2r+1} \cdot F(-\mu + r + 1, r+1, 2r+2, \xi). \tag{8.6}$$

Lemma b: If $\xi \neq 0$ we have

$$A_r(\xi) \cdot B_{r+1}(\xi) + B_r(\xi) \cdot A_{r+1}(\xi). \tag{8.7}$$

Lemma c: If $0 < \xi < 1$ then the following inequalities are true

$$0 < A_r(\xi) < 1, \quad 0 < C_r(\xi) < \xi^{2r+1} A_r(1). \tag{8.8}$$

Lemma d: With the marks above we have

$$\binom{2r}{r} A_r(1) = \prod_{m=1}^{r} \left(1 - \frac{\mu}{m}\right). \tag{8.9}$$

9. **Lemma e:** The coefficients of the polynomials $G_r(\xi)$ and $H_r(\xi)$ are integers.

Proof: According to (4.1) and (4.2) we have

$$G_r(\xi) = q_r n^r \sum_{m=0}^{r} \binom{r+\mu}{m} \binom{2r-m}{r} (-\xi)^m, \tag{9.1}$$

$$H_r(\xi) = q_r n^r \sum_{m=0}^{r} \binom{r-\mu}{m} \binom{2r-m}{r} (-\xi)^m. \tag{9.2}$$

So we must show that the two numbers

$$g_m = \prod_{l=1}^{r-m+1} (l \cdot n + k) \text{ and } h_m = \prod_{l=1}^{r-m+1} (l \cdot n - k)$$

are divisible by $m!:q_r$ and that for $m = 1, 2, \ldots r$. The general term in e.g. $G_r(\xi)$ can be written

$$q_r n^r \frac{(r+\mu)(r+\mu-1)\ldots(r+\mu-m+1)}{m!} \cdot N =$$

$$= q_r n^{r-m} \frac{(nr+k)(n[r-1]+k)\ldots(n[r-n+1]+k)}{m!} N$$

where N is an integer. According to the definition of q_r it is obviously sufficient to prove that every prime p with $(p, n) = 1$ is a divisor of g_m and h_m and further that the exponent of the highest power of p which divides g_m and h_m is $\leqslant$ the exponent of the highest power of p which divides $m!$. Among the numbers $1, 2, \ldots m$ exactly $\left[\frac{m}{p^\nu}\right]$ are divisible by p^ν. As the difference between two consecutive factors of the numerator is n and $(n, p^\nu) = 1$, at least $\left[\frac{m}{p^\nu}\right]$ factors are divisible by p^ν. Thus the theorem is proved.

Lemma f: Let $0 < \xi < 1$. For every positive integer r there are two polynomials $G_r(\xi)$ and $H_r(\xi)$ with integer coefficients such that the following inequalities hold

$$G_r(\xi) \cdot H_{r+1}(\xi) + H_r(\xi) \cdot G_{r+1}(\xi) \tag{9.3}$$

$$0 < G_r(\xi) < s_r \tag{9.4}$$

$$0 < G_r(\xi) - (1-\xi)^\mu H_r(\xi) < u_r \xi^{2r+1}. \tag{9.5}$$

Proof: The first inequality is an immediate consequence of Lemma b, and by Lemma c we obtain

$$0 < G_r(\xi) = s_r A_r(\xi) < s_r$$

and (9.4) is proved. According to (8.3), (8.4), (8.8) and (8.9) it follows

$$0 < G_r(\xi) - (1-\xi)^\mu H_r(\xi) = s_r C_r(\xi) < s_r \xi^{2r+1} A_r(1) =$$

$$= \binom{2r}{r} q_r n^r A_r(1) \xi^{2r+1} = u_r \xi^{2r+1}.$$

Lemma g: Let r be an arbitrary positive integer and $\lambda_n = 4\left(n \prod_{p/n} p^{\frac{1}{p-1}}\right)^n$ where p runs through all the different primes of n. The inequality

$$n s_{r+2} \left(\frac{u_r}{1 - \frac{k}{n}}\right)^{n-1} < \lambda_n^{r+1} \tag{9.6}$$

is true.

The proof is an immediate consequence of a corresponding theorem in Siegel's work. He proves

$$n s_{r+2} \left(\frac{t_r}{1 - \frac{1}{n}}\right)^{n-1} < \lambda_n^{r+1}$$

where

$$t_r = q_r n^r \prod_{m=1}^{r} \left(1 - \frac{1}{m \cdot n}\right).$$

Hence we see that (9.6) is true, for as $k \geqslant 1$ we have

$$\prod_{m=2}^{r} \left(1 - \frac{k}{m \cdot n}\right) \leqslant \prod_{m=2}^{r} \left(1 - \frac{1}{m \cdot n}\right).$$

§ 4. Proof that only one equation can be solvable

10. Let us consider two arbitrary Diophantine equations belonging to the same class of the field $K\left(\sqrt[n]{\frac{A_1}{B_1}}\right)$ and which are solvable with the solutions $x = x_i$, $y = y_i$; $x = x_j$ and $y = y_j$.

$$A_i x_i^n - B_i y_i^n = C_i \tag{10.1}$$

$$|A_j x_j^n - B_j y_j^n| = C_j. \tag{10.2}$$

In order to prove Theorem A it is evidently sufficient to prove that the supposition that both are solvable is a contradiction. We shall apply the results of the theorems concerning the hypergeometric functions to the inequalities of the lemmata in § 2.

Let us choose the number ξ

$$\xi = 1 - \frac{B_i}{A_i}\left(\frac{y_i}{x_i}\right)^n \tag{10.3}$$

and

$$(1-\xi)^{\frac{k}{n}} = \left[\sqrt[n]{\frac{B_i}{A_i}} \cdot \frac{y_i}{x_i}\right]^k. \tag{10.4}$$

According to (4.2) we have $0 < \xi < 1$, $\xi = \frac{C_i}{L_i}$. At first we consider the case $1 \leqslant k < \frac{n}{2}$ so that $\mu = \frac{k}{n} < \frac{1}{2}$ where μ is the number defined in § 3. Let further m be the positive integer mentioned in Lemma 4a and G_m and H_m be the polynomials with integer coefficients defined in the former paragraph.

By the relation (9.3) it is possible to choose a positive integer r, where $r = m$ or $m-1$ such that

$$\frac{q}{p}\frac{y_j}{x_j} G_r(\xi) - \left(\frac{y_i}{x_i}\right)^k H_r(\xi) \neq 0 \tag{10.5}$$

and p, q are the integers mentioned in (5.2). At first we treat the case $n \geqslant 6$ and $n = 5$, $k = 1$ i.e. according to the preceding Lemma 4a the number $m \geqslant 2$ and hence $r \geqslant 1$. The remaining cases ($n = 4$ and $n = 5$, $k = 2$ when $m = r = 1$) we treat separately in the next paragraph.

From Lemma f, (10.3) and (10.4) we obtain

$$0 < G_r(\xi) - \sqrt[n]{\left(\frac{B_i}{A_i}\right)^k}\left(\frac{y_i}{x_i}\right)^k H_r(\xi) < u_r\left(\frac{C}{L_i}\right)^{2r+1}$$

and according to (6.7) and (9.4) the inequality

$$\left| G_r(\xi) - \sqrt[n]{\frac{B_j}{A_j}}\frac{y_j}{x_j} G_r(\xi) \right| < s_r \frac{C}{L_j}$$

is valid, and it follows from the two last inequalities and the equation (5.2) that

$$\sqrt[n]{\left(\frac{B_i}{A_i}\right)^k}\left|\frac{q}{p}\frac{y_j}{x_j}G_r(\xi)-\left(\frac{y_i}{x_i}\right)^k H_r(\xi)\right|<s_r\frac{C}{L_j}+u_r\left(\frac{C}{L_i}\right)^{2r+1}.$$

The left-hand member is (except the first factor) the absolute value of a rational number, which is not zero by (10.5) and whose denumerator is a divisor of the number $p\,x_i^k\,x_j\,L_i^r$. Consequently the following inequality holds:

$$p\,x_i^k\,x_j\,L_i^r\sqrt[n]{\left(\frac{A_i}{B_i}\right)^k}\left\{s_r\frac{C}{L_j}+u_r\left(\frac{C}{L_i}\right)^{2r+1}\right\}>1$$

or since $p\leqq\sqrt[n]{A_j\,B_i^k}$

$$L_i^{\frac{k}{n}}L_j^{\frac{1}{n}}L_i^r\left\{s_r\frac{C}{L_j}+u_r\left(\frac{C}{L_i}\right)^{2r+1}\right\}>1. \tag{10.6}$$

This relation is impossible however. For as $r\leqq m$ it follows from Lemma 4a

$$L_i^{\frac{k}{n}}L_j^{\frac{1}{n}}L_i^r\,s_r\frac{C}{L_j}\leqq L_i^{\frac{k}{n}}L_j^{\frac{1}{n}}L_i^m\,s_m\frac{C}{L_j}\leqq\frac{k}{n} \tag{10.7}$$

and as $m\leqq r+1$, by the lemmata 4a and 5 and the inequalities (9.6) and (6.5) it follows

$$L_i^{k/n}\cdot L_j^{1/n}\cdot L_i^r\cdot u_r\left(\frac{C}{L_i}\right)^{2r+1}<C^{2r+1}\cdot u_r\cdot L_i^{-r-1+\frac{k}{n}}(n\,C\,s_{r+2}\,L_i^{r+2+\frac{k}{n}})^{\frac{1}{n-1}}\leqq$$

$$\leqq C^{2r+2}\,L_i^{-r-1+\frac{r+2+k}{n-1}}\left(1-\frac{k}{n}\right)\lambda_n^{\frac{r+1}{n-1}}\leqq\left(1-\frac{k}{n}\right)[C^{2n-2}\lambda_n L_i^{-n+\frac{5}{2}+\frac{k}{r+1}}]^{\frac{r+1}{n-1}}\leqq$$

$$\leqq\left(1-\frac{k}{n}\right)[C^{2n-2}\lambda_n L_i^{-\frac{3n}{4}+\frac{9}{4}}]^{\frac{r+1}{n-1}}\leqq\left(1-\frac{k}{n}\right)[C^{2n-2}\lambda_n T^{-\frac{3}{8}(n-3)}]^{\frac{r+1}{n-1}}\leqq 1-\frac{k}{n}.$$

By this inequality and (10.7) it follows that the left-hand member of (10.6) is <1 which is a contradiction.

We shall now treat the cases $n=4$ or 5 and $m\geqq 2$ i.e. $r\geqq 1$. First suppose that $n=4$. Then $k=1$ and the inequality (10.7) is still valid. Further

$$L_i^{k/n}\,L_j^{1/n}\,L_i^r\cdot u_r\left(\frac{C}{L_i}\right)^{2r+1}<\left(1-\frac{1}{n}\right)\cdot[C^{2n-2}\lambda_n L_i^{-n+\frac{5}{2}+\frac{1}{r+1}}]^{\frac{r+1}{n-1}}\leqq$$

$$\leqq\tfrac{3}{4}[C^6\lambda_4\cdot L_i^{-1}]^{\frac{r+1}{3}}\leqq\tfrac{3}{4}[C^6\cdot 4^7\cdot T^{-1/3}]^{\frac{r+1}{3}}\leqq\tfrac{3}{4}$$

according to (4.2).

Analogously for $n=5$, $k=1$ or 2:

$$L_i^{k/n} L_j^{1/n} L_i^r u_r \left(\frac{C}{L_i}\right)^{2r+1} < \left(1-\frac{k}{n}\right)(C^{2n-2}\lambda_n L_i^{-n+\frac{5}{2}+\frac{k}{r+1}})^{\frac{r+1}{4}} \leqslant$$

$$\leqslant \left(1-\frac{k}{n}\right)(C^8\lambda_5 T^{-\frac{3}{4}})^{\frac{r+1}{4}} \leqslant \left(1-\frac{k}{n}\right).$$

The relation (10.7) is still true.

Thus we have proved what was purposed.

Let us now consider the case $\frac{n}{2} < k < n$, $1 \leqslant k' < \frac{n}{2}$ and let m' be the natural number mentioned in Lemma 4 b and $G_{m'}(\xi)$ and $H_{m'}(\xi)$ the polynomials defined in § 3. We choose $r=m'-1$ or $r=m'$ such that the number

$$\frac{p'}{q'}\frac{x_j}{y_j} G_r(\xi) - \left(\frac{y_i}{x_i}\right)^{k'} H_r(\xi)$$

is different from zero, which is possible according to (9.3). p' and q' are the coprime integers mentioned in (6.16) and ξ is the number

$$\xi = 1 - \frac{B_i}{A_i}\left(\frac{y_i}{x_i}\right)^n = \frac{C_i}{L_i}$$

and thus

$$(1-\xi)^{\frac{k'}{n}} = \left(\sqrt[n]{\frac{B_i}{A_i}}\,\frac{y_i}{x_i}\right)^{k'}.$$

If $n \geqslant 6$ or $n=5$, $k'=1$ we have $r \geqslant 1$ and by (9.5)

$$0 < G_r(\xi) - \sqrt[n]{\left(\frac{B_i}{A_i}\right)^{k'}}\left(\frac{y_i}{x_i}\right)^{k'} H_r(\xi) < u_r\left(\frac{C}{L_i}\right)^{2r+1}$$

and according to (6.18) and (9.4)

$$\left| G_r(\xi) - \sqrt[n]{\frac{A_j}{B_j}}\,\frac{x_j}{y_j} G_r(\xi)\right| < s_r \frac{C}{L_j'}.$$

The last two inequalities and the relation (6.16) implies

$$\sqrt[n]{\left(\frac{B_i}{A_i}\right)^{k'}}\left|\frac{p'}{q'}\frac{x_j}{y_j} G_r(\xi) - \left(\frac{y_i}{x_i}\right)^{k'} H_r(\xi)\right| < s_r \frac{C}{L_j'} + u_r\left(\frac{C}{L_i}\right)^{2r+1}.$$

The denumerator of the left-hand member (except the n:th root) is a divisor of $q' x_i^{k'} y_j L_i^r$. Further the inequality $q' \leqslant \sqrt[n]{B_i^{k'} B_j}$ is true by (6.16). Hence

$$L_j'^{\frac{1}{n}} L_i^{\frac{k'}{n}} L_i^r \left\{ s_r \frac{C}{L_j'} + u_r \left(\frac{C}{L_i} \right)^{2r+1} \right\} > 1.$$

The rest of the proof evidently becomes just as the preceding proof.

The proofs of the cases $n = 4$ or 5 and $m' \geqslant 2$ are established in the same way as before.

Thus we have proved Theorem A for $n \geqslant 6$.

§ 5. Proof in the cases $n = 4$ and $n = 5$

11. Suppose at first that $n = 4$. Then $k = 1$ or 3. Only the case $m = r = 1$ is left; m is the number defined in Lemma 4. As in the preceding paragraph it is sufficient to establish a proof for $k = 1$. The case $k' = 1$ is then treated similarly. Thus it suffices to prove the impossibility of the relation

$$\frac{q}{p} \frac{y_j}{x_j} G_1(\xi) - \frac{y_i}{x_i} H_1(\xi) = 0. \tag{11.1}$$

The polynomials $G_1(\xi)$ and $H_1(\xi)$ are

$$G_1(\xi) = 8 - 5\xi, \quad H_1(\xi) = 8 - 3\xi$$

and according to (5.2)

$$\sqrt[4]{\frac{A_i}{B_i}} = \frac{q}{p} \sqrt[4]{\frac{A_j}{B_j}}$$

it follows from (11.1)

$$\sqrt[4]{\frac{A_i B_j}{A_j B_i}} \frac{y_j}{x_j} = \frac{y_i}{x_i} \cdot \frac{H_1(\xi)}{G_1(\xi)}.$$

Putting $\xi = \dfrac{C_i}{L_i}$ we obtain

$$\frac{B_j y_j^4}{A_j x_j^4} = \frac{B_i y_i^4}{A_i x_i^4} \left(\frac{8L_i - 3C_i}{8L_i - 5C_i} \right)^4 \tag{11.2}$$

and by the supposition $(A_j \cdot B_j, C_j) = 1$ we see that the numerator is prime to the denumerator of the left-hand member. Then there is a positive integer u such that

$$u A_j x_j^4 = A_i x_i^4 (8 L_i - 5 C_i)^4$$

and (11.3)

$$u B_j y_j^4 = B_i y_i^4 (8 L_i - 3 C_i)^4.$$

Hence

$$u (A_j x_j^4 - B_j y_j^4) = A_i x_i^4 (8 L_i - 5 C_i)^4 - B_i y_i^4 (8 L_i - 3 C_i)^4. \quad (11.4)$$

Simple calculations show that the right-hand member M is

$$M = C_i^3 (320 L_i^2 - 320 L_i C_i + 81 C_i^2) > 320 L_i. \quad (11.5)$$

However it is easy to see that since $(L_i, C_i) = 1$

$$(L_i, 8 L_i - 5 C_i) \leqslant 5$$

$$(L_i - C_i, 8 L_i - 3 C_i) \leqslant 5$$

$$(L_i, 8 L_i - 3 C_i) \leqslant 3$$

$$(L_i, L_i - C_i) = 1$$

$$(L_i - C_i, 8 L_i - 5 C_i) \leqslant 3$$

$$(8 L_i - 5 C_i, 8 L_i - 3 C_i) \leqslant 8$$

and consequently it follows by (11.3) that u is a divisor of a number $\leqslant 3 \cdot 5 \cdot 8^4$ and thus $u \leqslant 15 \cdot 8^4$. According to (11.4) and (11.5) we obtain

$$C_j \cdot 15 \cdot 8^4 \geqslant u (A_j x_j^4 - B_j y_j^4) > 320 L_i \quad (11.6)$$

and by (4.2) and (6.5) it follows

$$15 \cdot 8^4 C > 320 \cdot T^{n/4} \geqslant 320 \cdot 4^7 \cdot C^6$$

which is a contradiction and consequently (11.1) is impossible.

Analogously we perceive, that if $k = 3$ i.e. $k' = 1$ and

$$\frac{p'}{q'} \frac{x_j}{y_j} G_1(\xi) - \frac{y_i}{x_i} H_1(\xi) = 0$$

it follows

$$\frac{A_j x_j^4}{B_j y_j^4} = \frac{B_i y_i^4}{A_i x_i^4} \left(\frac{8 L_i - 3 C_i}{8 L_i - 5 C_i} \right)^4$$

and since $L_j' = B_j y_j^4$ the continued argumentation will be identical with the preceding one.

12. The case $n=5$, $k=2$ and 3 is left. Consider the case $k=2$; if $k=3$, k' is 2 and the argumentation will be analogous. Supposing

$$\frac{q}{p}\frac{y_j}{x_j}G_1(\xi)-\left(\frac{y_i}{x_i}\right)^k H_1(\xi)=0 \tag{12.1}$$

where

$$\xi=1-\frac{B_i}{A_i}\left(\frac{y_i}{x_i}\right)^5$$

and the polynomials

$$G_1(\xi)=10-7\xi \quad H_1(\xi)=10-3\xi$$

we obtain according to (12.1)

$$\frac{B_j y_j^5}{A_j x_j^5}=\left(\frac{B_i y_i^5}{A_i x_i^5}\right)^2\left(\frac{10L_i-3C_i}{10L_i-7C_i}\right)^5.$$

As $(A_j x_j^5,\ B_j y_j^5)=1$ by the connection between the numbers A_j, B_j and C_j, we can find a positive integer v, such that

$$v B_j y_j^5=(B_i y_i^5)^2(10L_i-3C_i)^5 \tag{12.2}$$

$$v A_j x_j^5=(A_i x_i^5)^2(10L_i-7C_i)^5. \tag{12.3}$$

By subtraction we obtain

$$\pm v C_j=(A_i x_i^5)^2(10L_i-7C_i)^5-(B_i y_i^5)^2(10L_i-3C_i)^5. \tag{12.4}$$

A computation of the right-hand member M gives

$$M=14000\,L_i^4C_i^3-28000\,L_i^3C_i^4+18536\,L_i^2C_i^5-4536\,L_iC_i^6+243\,C_i^7. \tag{12.5}$$

It is easy to verify that

$$(10L_i-7C_i,\ 10L_i-3C_i)\leqslant 10$$

$$(L_i,\ 10L_i-3C_i)\leqslant 3$$

$$(L_i,\ L_i-C_i)=1$$

$$(L_i-C_i,\ 10L_i-7C_i)\leqslant 3$$

and from (12.2) and (12.3) it follows that v is a divisor of a number that is $\leqslant 3^2\cdot 10^5$ and consequently $v\leqslant 9\cdot 10^5$.

But according to (12.5) we obtain

$$9\cdot 10^5 C\geqslant |vC_j|=|M|\geqslant 14000\,L_i^3C_i^3(L_i-2C_i)$$

which is impossible by (6.5) and (4.2).

Thus the proof of Theorem A is complete.

Remark 1: If $C=1$ and $L_i \geqslant 3^5$ then (12.1) is impossible. This fact is used in the proof of Theorem B.

Remark 2: It is possible to determine a sharper inequality than (3.2), $T^{\frac{n-5}{4}} \geqslant C^f n^{n+2}$. We can e.g. choose

$$T = C^{\frac{4f}{n-5}} \max \{[81 \cdot 2^{4(3-n)} n^{12} (n+1)^{4(n-1)}]^{\frac{1}{n-5}}, [4^{\frac{1}{n}} n \prod_{p/n} p^{\frac{1}{p-1}}]^{\frac{8n}{3(n-3)}}\}$$

with p running through all the different primes of n. What is interesting, however, is that the limit depends on n only.

§ 6. Diophantine equations of the third degree

13. As mentioned in the introduction (Theorem III, p. 6) Nagell [13] has treated this problem in the case $n=3$ and $C_\nu = 1$ or 3 for all ν. With the method shaped here it is not possible to establish a proof for a general C_ν, but in the special case $C_\nu = 1$ for all ν we can prove the following theorem:

Theorem AA: Let A_ν and B_ν be coprime positive integers containing no cube of a prime. Among all the Diophantine equations

$$|A_\nu x^3 - B_\nu y^3| = 1 \quad (\nu = 1, 2, \ldots) \tag{13.1}$$

belonging to the same class and where

$$\min_{\nu=1,2,\ldots} A_\nu \cdot B_\nu = T$$

and

$$T^{1/6} > 747 \tag{13.2}$$

there is at most one which is solvable in positive integers x and y.

It is of interest to see that a result similar to that of Nagell [13] can be received by quite different methods.

The proofs in this case $n=3$ are analogous to those which are furnished in the other cases. We suppose that two of the Diophantine equations (13.1) are solvable. As $n=3$, k must have the value 1 or 2 and according to the preceding argumentation it is sufficient to treat the value $k=1$, for the proofs when $k=2$ are analogous.

Let us use the same marks as before and with the suppositions (6.3) and (6.4) the following lemmata are true:

Lemma 3c: The following inequalities are valid:

$$L_i > T^{3/2} \tag{13.3}$$

$$L_j > 27\,(L_i - 1)^2. \tag{13.4}$$

Lemma 4c: There is a unique positive integer m such that

$$s_m L_i^m \leqslant \tfrac{7}{10} L_i^{-\frac{1}{2}} L_j^{\frac{3}{2}} < s_{m+1} L_i^{m+1}. \tag{13.5}$$

Proof of 3c: The proof of (13.3) is immediately clear.
We have

$$1 - \sqrt[3]{\frac{B_i}{A_i}}\,\frac{y_i}{x_i} < \frac{1}{3} \cdot \frac{1}{(A_i x_i^3)^{2/3}} \cdot \frac{1}{(B_i y_i^3)^{1/3}} \tag{13.6}$$

and

$$\left| 1 - \sqrt[3]{\frac{B_j}{A_j}}\,\frac{y_j}{x_j} \cdot \right| < \frac{1}{3} \cdot \frac{1}{(A_j x_j^3)^{2/3}} \cdot \frac{1}{(B_j y_j^3)^{1/3}} \tag{13.7}$$

for

$$\frac{1}{\sqrt[3]{A_i}\,x_i - \sqrt[3]{B_i}\,y_i} = (\sqrt[3]{A_i}\,x_i)^2 + \sqrt[3]{A_i B_i}\,x_i y_i + (\sqrt[3]{B_i}\,y_i)^2 \geqslant 3\sqrt[3]{A_i}\,x_i \cdot \sqrt[3]{B_i}\,y_i.$$

It is easily seen since $B_j y_j^3 = L_j \pm 1$ that the right-hand member of (13.7) is $\leqslant L_j^{-1}$. From this inequality, (5.2) and the relation (13.6) it follows

$$\sqrt[3]{\frac{B_i}{A_i}}\,\frac{|p\,x_j y_i - q\,x_i y_j|}{p\,x_i x_j} < \frac{1}{3}\,\frac{1}{L_i^{2/3}} \cdot \frac{1}{(L_i - 1)^{1/3}} + \frac{1}{L_j}.$$

As was proved in Lemma 3a, the numerator of the left-hand member is not zero. Furthermore $p \leqslant \sqrt[3]{A_j B_i}$ by (5.2) and we obtain

$$\frac{1}{L_i^{1/3} L_j^{1/3}} < \frac{1}{3}\,\frac{1}{L_i^{2/3}(L_i - 1)^{1/3}} + \frac{1}{L_j}$$

or

$$1 < \frac{1}{3}\,\frac{L_j^{1/3}}{L_i^{1/3}(L_i - 1)^{1/3}} + \frac{L_i^{1/3}}{L_j^{2/3}}. \tag{13.8}$$

The inequality does not hold for $L_j = L_i - 1$ as $L_i \geqslant 4$ according to (13.2) and (13.3). Nor does it for $L_j = 27\,(L_i - 1)^2$, for putting it into the right-hand member we obtain

$$\left(1 - \frac{1}{L_i}\right)^{1/3} + \frac{L_i^{1/3}}{9\,(L_i - 1)^{4/3}} < 1 - \frac{1}{3\,L_i} + \frac{1}{3\,L_i} = 1.$$

Observing that the right-hand member of (13.8) is a convex function of $L_j^{\frac{1}{3}}$ it follows that the inequality (13.4) is true.

Proof of Lemma 4 c: It is evidently sufficient to prove, that

$$s_1 L_i \leqslant \frac{7}{10} L_i^{-1/3} L_j^{4/3}.$$

With regard to (13.4) and the fact that $s_1 = 6$ for $n = 3$ we obtain

$$\frac{7}{60} L_j^{4/3} L_i^{-4/3} > \frac{21}{20}\left(1 - \frac{1}{L_i}\right)^{4/3} \geqslant 1$$

since $L_i > 28$ by (13.2).

Now choose

$$\xi = 1 - \frac{B_i}{A_i}\left(\frac{y_i}{x_i}\right)^3 \tag{13.9}$$

i.e.

$$\sqrt[3]{1-\xi} = \sqrt[3]{\frac{B_i}{A_i}}\,\frac{y_i}{x_i}$$

where $0 < \xi < 1$ and $\xi = L_i^{-1}$. The positive integer m defined in Lemma 4 c is at first supposed to be $\geqslant 2$. According to (9.3) it is possible to decide a natural number r such that $r = m$ or $r = m - 1$ such that

$$\frac{q}{p}\frac{y_j}{x_j} G_r(\xi) - \frac{y_i}{x_i} H_r(\xi) \tag{13.10}$$

is different from zero. Analogously to the preceding cases we obtain

$$0 < G_r(\xi) - \sqrt[n]{\frac{B_i}{A_i}}\,\frac{y_i}{x_i} H_r(\xi) < u_r\left(\frac{1}{L_i}\right)^{2r+1}$$

and

$$\left| G_r(\xi) - \sqrt[n]{\frac{B_j}{A_j}}\,\frac{y_j}{x_j} G_r(\xi) \right| < s_r \frac{1}{L_j}$$

Hence

$$\left| \frac{q}{p}\frac{y_j}{x_j} G_r(\xi) - \frac{y_i}{x_i} H_r(\xi) \right| < \sqrt[3]{\frac{A_i}{B_i}} \left\{ s_r \frac{1}{L_j} + u_r \left(\frac{1}{L_i}\right)^{2r+1} \right\}.$$

According to (13.10) the left-hand member is the absolute value of a rational number different from zero and whose denumerator is dividing $p x_i x_j L_i^r$, why

$$p x_i x_j L_i^r \sqrt[3]{\frac{A_i}{B_i}} \left\{ s_r \frac{1}{L_j} + u_r \left(\frac{1}{L_i}\right)^{2r+1} \right\} > 1.$$

Introducing $p \leqslant \sqrt[3]{A_j B_i}$ we obtain

$$L_i^{1/3} L_j^{1/3} L_i^r \left\{ s_r \frac{1}{L_j} + u_r \left(\frac{1}{L_i}\right)^{2r+1} \right\} > 1.$$

By Lemma 4 c it follows since $r \leqslant m$

$$L_i^{1/3} L_j^{1/3} L_i^r \, s_r \frac{1}{L_j} \leqslant L_i^{1/3} L_j^{1/3} L_i^m \, s_m \frac{1}{L_j} \leqslant \frac{7}{10}.$$

Supposing $m = r = 1$ and that (13.10) is not zero, we obtain according to Lemma 4 c

$$L_i^{1/3} L_j^{1/3} L_i^r \, u_r \left(\frac{1}{L_i}\right)^{2r+1} < 12 \cdot \sqrt{\frac{15}{7}} L_i^{-\frac{1}{2}} \leqslant \frac{3}{10}$$

if $L_i \geqslant 3430$. The case $m = 1$ and the relation (13.10) is zero will be separately treated below. Furthermore if $m = 2$ we choose $r = 2$; in fact the relation (13.10) is different from zero for $r = 2$ which is simply derived in 15 below. So we may suppose that $m \geqslant 3$, $r \geqslant 2$. According to (9.6) and Lemma 4 c as $m \leqslant r+1$ we obtain

$$L_i^{1/3} L_j^{1/3} L_i^r \, u_r \left(\frac{1}{L_i}\right)^{2r+1} < u_r L_i^{-\frac{r-1}{2}} \left(\frac{10}{7} s_{r+2}\right)^{1/3} <$$

$$< \frac{2\sqrt{30}}{9\sqrt{7}} L_i^{-\frac{r-1}{2}} \lambda_3^{\frac{r+1}{2}} \leqslant \frac{2\sqrt{30}}{9\sqrt{7}} (T^{-1/6} \lambda_3)^{\frac{r+1}{2}} \leqslant \frac{3}{10}$$

which is easy to see. With this our proof is finished except two special cases.

14. Suppose that $m = 2$ and prove that the relation (13.10) is different from zero. Let us thus suppose that

$$\frac{q}{p} \frac{y_j}{x_j} G_2(\xi) = \frac{y_i}{x_i} H_2(\xi). \tag{14.1}$$

According to the definitions of the polynomials $G_2(\xi)$ and $H_2(\xi)$ we have

$$G_2(\xi) = 54 - 63\,\xi + 14\,\xi^2$$

$$H_2(\xi) = 54 - 45\,\xi + 5\,\xi^2.$$

and introducing (5.2) in (14.1) we obtain

$$\frac{\sqrt[3]{A_i B_j}}{\sqrt[3]{A_j B_i}} \cdot \frac{y_j}{x_j} = \frac{y_i}{x_i} \frac{H_2(\xi)}{G_2(\xi)}$$

and with $\xi = L_i^{-1}$

$$\frac{B_j y_j^3}{A_j x_j^3} = \frac{B_i y_i^3}{A_i x_i^3} \left(\frac{54 L_i^2 - 45 L_i + 5}{54 L_i^2 - 63 L_i + 14} \right)^3 .$$

Since $(A_j x_j^3, B_j y_j^3) = 1$ according to the definitions of A_j, B_j, C_j we can determine a positive integer u such that

$$u A_j x_j^3 = A_i x_i^3 (54 L_i^2 - 63 L_i + 14)^3 \tag{14.2}$$

and

$$u B_j y_j^3 = B_i y_i^3 \ (54 L_i^2 - 45 L_i + 5)^3 .$$

Hence

$$\pm u = L_i (54 L_i^2 - 63 L_i + 14)^3 - (L_i - 1)(54 L_i^2 - 45 L_i + 5)^3 \tag{14.3}$$

Combining the inequality (13.4) with the relation (14.2) we obtain

$$u = \frac{L_i (54 L_i^2 - 63 L_i + 14)^3}{L_j} \leqslant \frac{L_i \cdot 54^3 (L_i^2 - 1)^3}{27 (L_i - 1)^2} = 2 \cdot 54^2 L_i (L_i + 1)^3 (L_i - 1) .$$

From (14.3) we obtain another inequality for u. By a simple calculation we get

$$u > 12 \cdot 9^4 L_i^5 - 232 \cdot 9^3 L_i^4 .$$

From these two last inequalities it follows

$$2 L_i (L_i + 1)^3 (L_i - 1) > 27 L_i^5 - 58 L_i^4$$

which is a contradiction since $L_i > 3$. Thus the supposition of (14.1) leads to a contradiction.

15. Finally suppose that (13.10) is zero for $r = 1$ i.e.

$$\frac{q}{p} \frac{y_j}{x_j} G_1(\xi) = \frac{y_i}{x_i} H_1(\xi). \tag{15.1}$$

For $n = 3$ we have

$$G_1(\xi) = 3 - 2\xi, \quad H_1(\xi) = 3 - \xi$$

and analogously to the preceding proof it follows

$$\frac{B_j y_j^3}{A_j x_j^3} = \frac{B_i y_i^3}{A_i x_i^3} \left(\frac{3 L_i - 1}{3 L_i - 2} \right)^3 .$$

There is a natural number v such that

$$v A_j x_j^3 = A_i x_i^3 (3 L_i - 2)^3 \tag{15.2}$$

and

$$v B_j y_j^3 = B_i y_i^3 (3 L_i - 1)^3.$$

By subtraction

$$\pm v = L_i (3 L_i - 2)^3 - (L_i - 1)(3 L_i - 1)^3 = 2 L_i - 1. \tag{15.3}$$

But it is easily seen that $(2 L_i - 1, L_i) = 1$ and $(2 L_i - 1, 3 L_i - 2) = 1$. Consequently it follows by (15.2) that $v = 1$ and thus $L_i = 1$ which is a contradiction. Therefore the relation (15.1) does not hold and the proof of Theorem AA is complete.

§ 7. Proofs of Theorem B and Theorem C

16. It is now rather easy to prove the remaining theorems. Introducing $C_\nu = 1$ for all ν in the Diophantine equations we can sharpen the results in some adequate proofs. Consider the Diophantine equations belonging to the same class

$$\begin{aligned} |A_i x^n - B_i y^n| &= 1 \\ |A_j x^n - B_j y^n| &= 1 \end{aligned} \tag{16.1}$$

and which are solvable in positive integers; $x = x_i$, $y = y_i$ resp. $x = x_j$, $y = y_j$. Put $L_i = \max(A_i x_i^n, B_i y_i^n)$ e.g. $L_i = A_i x_i^n$. Since the equations above belong to the same class it follows

$$\sqrt[n]{\frac{A_j}{B_j}} = \frac{p}{q} \sqrt[n]{\left(\frac{A_i}{B_i}\right)^k} \tag{16.2}$$

and we can suppose $(p, q) = 1$, $1 \leqslant k < \frac{n}{2}$. It is unnecessary to treat the case $\frac{n}{2} < k < n$ as the argumentation is similar to the case $1 \leqslant k < \frac{n}{2}$. Furthermore we have treated both the cases in the proofs of Theorem A.

We suppose that $L_j \geqslant L_i$ with $L_j = A_j x_j^n$ and establish the following result:

Lemma 3 d: The inequality

$$L_j > \left(\frac{n}{k}\right)^n (L_i - 1)^{n-k} \tag{16.3}$$

is true, if $L_i \geqslant 3$, $n \geqslant 5$.

Proof. It is easily seen that

$$1 - \sqrt[n]{\left(\frac{B_i}{A_i}\right)^k \left(\frac{y_i}{x_i}\right)^k} \leqslant k\left(1 - \sqrt[n]{\frac{B_i}{A_i}\,\frac{y_i}{x_i}}\right)$$

and

$$\frac{1}{\sqrt[n]{A_i}\,x_i - \sqrt[n]{B_i}\,y_i} = (A_i x_i^n)^{\frac{n-1}{n}} + \ldots + (B_i y_i^n)^{\frac{n-1}{n}} > n\,(A_i x_i^n)^{\frac{n-1}{2n}} (B_i y_i^n)^{\frac{n-1}{2n}}$$

and

$$1 - \sqrt[n]{\left(\frac{B_i}{A_i}\right)^k \left(\frac{y_i}{x_i}\right)^k} < \frac{k}{n\,L_i^{\frac{n+1}{2n}} (L_i - 1)^{\frac{n-1}{2n}}}. \tag{16.4}$$

In the same way we get

$$\left|1 - \sqrt[n]{\frac{B_j}{A_j}\,\frac{y_j}{x_j}}\right| \leqslant \frac{1}{n\,L_j^{\frac{n+1}{2n}} (L_j \pm 1)^{\frac{n-1}{2n}}} < \frac{1}{L_j}. \tag{16.5}$$

With an analogous argumentation as in Lemma 3 c it follows from (16.4) and (16.5)

$$\frac{1}{L_i^{k/n} L_j^{1/n}} < \frac{k}{n\,L_i^{\frac{n+1}{2n}} (L_i - 1)^{\frac{n-1}{2n}}} + \frac{1}{L_j}$$

or

$$1 < \frac{k\,L_j^{1/n}}{n\,L_i^{\frac{n+1-2k}{2n}} (L_i - 1)^{\frac{n-1}{2n}}} + \frac{L_i^{k/n}}{L_j^{1-1/n}}. \tag{16.6}$$

The right-hand member of this inequality is a convex function of $L_j^{1/n}$ and the inequality does not hold for $L_j = L_i$, for putting this value in the right-hand member, we obtain

$$\frac{k}{n} \frac{L_i^{\frac{2k+1-n}{2n}}}{(L_i - 1)^{\frac{n-1}{2n}}} + \frac{1}{L_i^{1-\frac{k+1}{n}}} \leqslant \frac{k}{n} \frac{1}{(L_i - 1)^{\frac{n-1}{2n}}} + \frac{1}{L_i^{\frac{n-1}{2n}}} < 1$$

for $L_i \geqslant 3$, $n \geqslant 5$ and $k \leqslant \frac{n-1}{2}$. Neither the inequality is true for

$L_j = \left(\frac{n}{k}\right)^n (L_i - 1)^{n-k}$. Putting this value in the right-hand member of (16.6) it follows

$$\left(1 - \frac{1}{L_i}\right)^{\frac{n+1-2k}{2n}} + \left(\frac{k}{n}\right)^{n-1} \frac{L_i^{k/n}}{(L_i - 1)^{(n-k)\left(1-\frac{1}{n}\right)}} \leqq \left(1 - \frac{1}{L_i}\right)^{\frac{1}{n}} + \frac{1}{n L_i} < 1.$$

Consequently the inequality (16.3) is true, which was to be proved.

17. We suppose that none of the equations (16.1) has the solution $x = y = 1$. Consequently we have $L_i \geqq 2^n$ and if we suppose that none of the equations has the solution $x = 1$, $y = 2$ or $x = 2$, $y = 1$ if $5 \leqq n \leqq 7$ it follows $L_i \geqq 3^n$ for $5 \leqq n \leqq 7$.

The following theorem is easily obtained:

Lemma 4 d: There is a unique positive integer m such that

$$s_m L_i^m \leqq \frac{k}{n} L_i^{-\frac{k}{n}} L_j^{1-\frac{1}{n}} < s_{m+1} L_i^{m+1} \tag{17.1}$$

and $m \geqq 3$ if $n \geqq 8$ and $m \geqq 2$ if $n \geqq 6$ and if $n = 5$, $k = 1$.

Proof: According to Lemma 3 d we obtain if $n \geqq 8$, $s_3 = 20\,(n, 6)\,n^3$

$$\frac{k \cdot L_j^{\frac{n-1}{n}} L_i^{-3-\frac{k}{n}}}{n \cdot 20\,(n, 6) \cdot n^3} \geqq$$

$$\geqq \left(\frac{n}{k}\right)^{n-2} \cdot \left(1 - \frac{1}{L_i}\right)^{3+\frac{k}{n}} \frac{(L_i - 1)^{n-k-4}}{20 \cdot (n, 6)\, n^3} \geqq 0.9 \left(\frac{n}{k}\right)^{n-2} \frac{2^n - 1}{20 \cdot (n, 6) \cdot n^3}.$$

Now we evidently have

$$0.9 \left(\frac{8}{3}\right)^6 (2^8 - 1) > 20 \cdot 2 \cdot 8^3$$

$$0.9 \left(\frac{9}{4}\right)^7 (2^9 - 1) > 60 \cdot 9^3$$

$$0.9 \cdot \left(\frac{2n}{n-1}\right)^{n-2} (2^n - 1) > 120\, n^3 \text{ if } n \geqq 10.$$

The remaining cases $n = 5$, $k = 1$ and $n = 6$ or 7 are an immediate consequence of Lemma 4 a putting $C = 1$ in (7.1).

Thus Lemma 4 d is proved.

18. Comparing these reasonings with those in § 4 one can see easily that if the inequality

$$H = u_r L_i^{-r-1+\frac{k}{n}} (n s_{r+2} L_i^{r+2+\frac{k}{n}})^{\frac{1}{n-1}} \leqslant 1 - \frac{k}{n} \tag{18.1}$$

is still true, then the equations (16.1) cannot both be solvable. According to (9.6) we obtain

$$H < L_i^{-r-1+\frac{k}{n}+\frac{r+2+\frac{k}{n}}{n-1}} \cdot \lambda_n^{\frac{r+1}{n-1}} \left(1 - \frac{k}{n}\right).$$

Consequently (18.1) holds if

$$L_i^{r+1-\frac{k}{n}-\frac{r+2+\frac{k}{n}}{n-1}} > \lambda_n^{\frac{r+1}{n-1}}. \tag{18.2}$$

Introducing a function $g(n, k, r)$ such that

$$g(n, k, r) = 1 - \frac{k}{n(r+1)} - \frac{r+2+\frac{k}{n}}{(r+1)(n-1)}$$

we obtain since $r \geqslant 2$ if $n \geqslant 8$ that $g(n, k, r) \geqslant \frac{2}{3}$, $g(7, k, r) \geqslant \frac{1}{2}$, $g(6, 1, r) \geqslant \frac{3}{5}$, $g(5, 1, r) \geqslant \frac{1}{2}$, $g(5, 2, r) \geqslant \frac{3}{8}$.

Further

$$\lambda_n \leqslant 2^{2+\frac{n}{2}} n^{\frac{3n}{2}}$$

and for $n \geqslant 10$ the inequality

$$2^{\frac{2n}{3}} > 2^{\frac{4+n}{2(n-1)}} n^{\frac{3n}{2(n-1)}}$$

is valid, which is easy to verify. We have $\lambda_8 = 2^{34}$, $\lambda_9 = 4 \cdot 3^{22.5}$ and

$$2^{\frac{16}{3}} > 2^{\frac{34}{7}}, \qquad 2^{\frac{18}{3}} > 4^{\frac{1}{8}} \cdot 3^{\frac{22.5}{8}}.$$

Thus the proof is finished if $n \geqslant 8$.

Suppose that $n = 7$ or 6. Then we have $\lambda_7 = 4 \cdot 7^{\frac{49}{6}}$, $\lambda_6 = 2^{14} \cdot 3^9$ and

$$3^{\frac{7}{2}} > 4^{\frac{1}{6}} \cdot 7^{\frac{49}{36}}$$

$$3^{\frac{3 \cdot 6}{5}} > 2^{\frac{14}{5}} \cdot 3^{\frac{9}{5}}.$$

According to the proof in § 5 (Remark 1, p. 30) it is sufficient to prove that the inequality (18.1) is valid even for $n=5$, $r \geqslant 1$. Suppose at first that $r=1$. We have

$$u_1 = n-k \qquad s_3 = 20 \cdot 5^3.$$

Hence

$$H \leqslant (5-k)\, L_i^{-\frac{3}{4}} (20 \cdot 5^4)^{\frac{1}{4}} \leqslant 5^2 \cdot 3^{-\frac{15}{4}} \cdot 20^{\frac{1}{4}} \left(1-\frac{k}{5}\right) < 1-\frac{k}{5}.$$

For $r=2$ we have

$$u_2 = (n-k)\left(n-\frac{k}{2}\right) \qquad s_4 = 70 \cdot 5^4$$

and

$$H \leqslant (5-k)\left(5-\frac{k}{2}\right) L_i^{-\frac{3}{2}} (70 \cdot 5^5)^{\frac{1}{4}} \leqslant 22.5\, (70 \cdot 5^5)^{\frac{1}{4}} \cdot 3^{-\frac{15}{2}} \left(1-\frac{k}{5}\right) < 1-\frac{k}{5}.$$

At last we have for $r \geqslant 3$, $g(5, k, r) \geqslant \frac{9}{16}$, $\lambda_5 = 4 \cdot 5^{\frac{25}{4}}$ and

$$3^{\frac{9 \cdot 5}{16}} > 4^{\frac{1}{4}} \cdot 5^{\frac{25}{16}}.$$

Thus we have proved the second part of Theorem B.

However, $L_i \geqslant 3$ if we do not take into consideration the equation $|x^n - 2y^n| = 1$, and consequently there cannot be three solvable equations belonging to the same class. For according to Lemma 3 d we have

$$L_j > \left(\frac{n}{k}\right)^n 2^{n-k} > 2^n$$

and by a simple calculation we see that $L_j > 3^n$ for $n = 5$, 6 or 7 and this is sufficient to have the proof of Theorem B complete.

19. At last we suppose that the two Diophantine equations

$$\begin{aligned} |x^n - M^g y^n| &= 1 \\ |x^n - M^h y^n| &= 1 \end{aligned} \tag{19.1}$$

both are solvable in positive integers (x_g, y_g) resp. (x_h, y_h) and that g and h are natural numbers, $1 \leqslant g < n$, $1 \leqslant h < n$ and $(n, g) = (n, h) = 1$. We do not take into consideration equations belonging to the following classes: $K(\sqrt[n]{2})$, $(\sqrt[5]{31})$, $K(\sqrt[5]{33})$, $K(\sqrt[6]{63})$, $K(\sqrt[6]{65})$, $K(\sqrt[7]{127})$,

$K(\sqrt[7]{129})$. Let us further suppose that the first equation is solvable for $+1$ i.e.

$$x_g^n - M^g y_g^n = 1.$$

We introduce $M^g = m_1^n N_1$ and $M^h = m_2^n N_2$ where N_1 and N_2 does not contain the n:th power of a prime. We obtain

$$x_g^n - N_1 (m_1 y_g)^n = 1$$

$$\left| x_h^n - N_2 (m_2 y_h)^n \right| = 1.$$

There is a natural number k which is uniquely determined such that

$$h - g k \equiv 0 \pmod{n}$$

$$1 \leqslant k < n$$

and

$$\sqrt[n]{N_2} = \frac{1}{m_2} \sqrt[n]{M^h} = \frac{m}{m_2} \sqrt[n]{M^{gk}} = \frac{p}{q} \sqrt[n]{N_1^k}$$

where m, p and q are positive integers. The equations (19.1) thus belong to the same class and by Theorem B and the fact that we do not take into consideration equations belonging to the classes mentioned above, Theorem C follows.

Chapter II

ON THE DIOPHANTINE EQUATION $Ax^n - By^n = C$, $n = 3$ OR 4 IN CERTAIN IMAGINARY QUADRATIC FIELDS

§ 1. Definitions and theorem

20. Let n be one of the numbers 3 or 4 and $m = 3$ for $n = 3$ and $m = 1$ for $n = 4$, and let A, B and C be integers belonging to the quadratic field $K(\sqrt{-m})$. We shall establish an analogon of Thue-Siegels theorem concerning the maximum number of integral solutions of (1.1) in the cases $n = 3$ or 4 and consider the Diophantine inequality

$$|Ax^n - By^n| \leqslant |C|. \tag{20.1}$$

If x and y are integers belonging to $K(\sqrt{-m})$ which satisfy (20.1) we say that (x, y) is a solution of (20.1).

Every integer of the field $K(\sqrt{-m})$ can be written

$$a + b\theta$$

with $\theta = \sqrt{-1} = i$ (= the imaginary unit) if $m = 1$,

and $\theta = \varrho \left(= -\frac{1}{2} + \frac{\sqrt{-3}}{2} \right)$ if $m = 3$, and where a and b are rational integers.

The purpose of this chapter is to prove the following theorem:

Theorem D: Consider the Diophantine inequality

$$|Ax^n - By^n| \leqslant |C|, \quad n = 3 \text{ or } 4 \tag{20.2}$$

where A, B and C are integers of the field $K(\sqrt{-m})$ with $m = 3$ if $n = 3$ and $m = 1$ if $n = 4$, that satisfy the conditions: $(A, B) = 1$, $\sqrt[n]{\left|\frac{A}{B}\right|^2}$ is no rational number. Suppose further that

$$M = |AB| \geqslant \begin{cases} 16 \cdot 3^9 |C|^8 & n = 3 \\ 4^7 \cdot |C|^6 & n = 4 \end{cases} \tag{20.3}$$

Then the Diophantine inequality has none or eighteen associated solutions in relatively prime integers $x, y \in K(\sqrt{-3})$ for $n=3$ and none or sixteen associated solutions in relatively prime integers $x, y \in K(\sqrt{-1})$ if $n=4$.—Two solutions (x, y) and (x_1, y_1) are called associated if there is a relation $x=\varepsilon_1 \cdot x_1$, $y=\varepsilon_2 \cdot y_1$ where ε_1 and ε_2 are arbitrary units of the field we look at.

§ 2. The quadratic fields $K(\sqrt{-1})$ and $K(\sqrt{-3})$

21. Every integer of the field $K(\sqrt{-1})$ can be written

$$a+b \cdot i$$

where a and b are rational integers. If (x, y) is a solution of (20.2) (for $n=4$) then the associated solutions are $(\varepsilon_1 x, \varepsilon_2 y)$ with ε_1 and ε_2 arbitrary units of $K(\sqrt{-1})$. The units are ± 1, $\pm i$. We divide the possible combinations of the units $(\varepsilon_1, \varepsilon_2)$ into four classes L_1, L_2, L_3 and L_4:

$$L_1\colon\ (1, 1), (-1, -1), (i, i), (-i, -i)$$
$$L_2\colon\ (1, i), (-1, -i), (i, -1), (-i, 1)$$
$$L_3\colon\ (1, -1), (-1, 1), (i, -i), (-i, i)$$
$$L_4\colon\ (1, -i), (-1, i), (i, 1), (-i, -1).$$

These combinations are evidently the only possible ones and we observe that all the combinations satisfy (20.2) i.e. if (x, y) is a solution of (20.2), then there are together sixteen solutions of (20.2). The solution (x, y) is uniquely determined if we choose

$$\begin{aligned} 0 \leqslant \arg x < \frac{\pi}{2}, \\ 0 \leqslant \arg y < \frac{\pi}{2}. \end{aligned} \tag{21.1}$$

22. In the field $K(\sqrt{-3})$ the integers have the form

$$a+b \cdot \varrho$$

with $\varrho = \frac{1}{2}(-1+i\sqrt{3})$ and the units of the field are $\pm\varrho$, $\pm\varrho^2$ except ± 1. The different possibilities for the units can suitably be brought together in the six classes $L_1, \ldots, L_6$:

$$L_1\colon\ (1,1),\ (-1,-1),\ (\varrho,\varrho),\ (-\varrho,-\varrho),\ (\varrho^2,\varrho^2),\ (-\varrho^2,-\varrho^2)$$
$$L_2\colon\ (1,\varrho),\ (-1,-\varrho),\ (\varrho,\varrho^2),\ (-\varrho,-\varrho^2),\ (\varrho^2,1),\ (-\varrho^2,-1)$$
$$L_3\colon\ (1,\varrho^2),\ (-1,-\varrho^2),\ (\varrho,1),\ (-\varrho,-1),\ (\varrho^2,\varrho),\ (-\varrho^2,-\varrho)$$
$$L_4\colon\ (1,-1),\ (-1,1),\ (\varrho,-\varrho),\ (-\varrho,\varrho),\ (\varrho^2,-\varrho^2),\ (-\varrho^2,\varrho^2)$$
$$L_5\colon\ (1,-\varrho),\ (-1,\varrho),\ (\varrho,-\varrho^2),\ (-\varrho,\varrho^2),\ (\varrho^2,-1),\ (-\varrho^2,1)$$
$$L_6\colon\ (1,-\varrho^2),\ (-1,\varrho^2),\ (\varrho,-1),\ (-\varrho,1),\ (\varrho^2,-\varrho),\ (-\varrho^2,\varrho)$$

There are no more combinations than these above. If (x, y) is a solution of (20.2) for $n=3$ it is immediately clear that $(-x, -y)$, $(\varrho x, \varrho y)$, $(-\varrho x, -\varrho y)$, $(\varrho^2 x, \varrho^2 y)$ and $(-\varrho^2 x, -\varrho^2 y)$ are solutions too. We say that L_1 is a solution of (20.2) in this case. Suppose L_1 is a solution of (20.2). Then L_2 and L_3 are solutions too, but not L_4, L_5 and L_6. For suppose that L_1 and L_4 are solutions. We obtain

$$|Ax^3 - By^3| \leqq |C|$$
$$|Ax^3 + By^3| \leqq |C|$$

Hence

$$2|C|^2 \geqq |Ax^3 - By^3|^2 + |Ax^3 + By^3|^2 = 2|Ax^3|^2 + 2|By^3|^2 \geqq 4M^{1/3}$$

which is a contradiction according to (20.3). Analogous proofs can evidently be furnished in the remaining cases. Consequently there are another seventeen solutions if there is one. A possible solution (x, y) of (20.2) is thus uniquely determined if we choose

$$\begin{aligned} 0 &\leqq \arg x < \frac{\pi}{3} \\ -\frac{\pi}{3} &\leqq \arg y < \frac{\pi}{3}. \end{aligned} \tag{22.1}$$

In the sequel we mean by a solution (x, y) the numbers x, y satisfying the inequalities (21.1) resp. (22.1).

§ 3. Hypergeometric functions

23. Consider the hypergeometric polynomials

$$A_r(z) = F(-\nu - r, -r, -2r, z) =$$
$$= \sum_{m=0}^{r} \frac{(r+\nu)(r+\nu-1)\ldots(r+\nu-m+1)}{2r(2r-1)\ldots(2r-m+1)} \binom{r}{m} (-z)^m$$

$$B_r(z) = F(\nu - r, -r, -2r, z) =$$

$$= \sum_{m=0}^{r} \frac{(r-\nu)(r-\nu-1)\dots(r-\nu-m+1)}{2r(2r-1)\dots(2r-m+1)} \binom{r}{m} (-z)^m$$

where the function

$$F(\alpha, \beta, \gamma, z) = 1 + \frac{\alpha \cdot \beta}{1 \cdot \gamma} \cdot z + \cdots$$

satisfies the differential equation

$$z(z-1)\frac{d^2F}{dz^2} + \{(1+\alpha+\beta)z - \gamma\}\frac{dF}{dz} + \alpha \cdot \beta \cdot F = 0$$

and z is an arbitrary complex number with the modulus < 1. Further we put

$$C_r(z) = A_r(z) - (1-z)^{\nu} B_r(z) \tag{23.1}$$

with $\nu = \frac{1}{n}$ and choose the principal branch of $\sqrt[n]{1-z}$.

According to Siegel [15] the following theorems are true:

I. There is a constant $\varrho_r \neq 0$ such that

$$C_r(z) = \varrho_r z^{2r+1} F(-\nu + r + 1, r+1, 2r+2, z). \tag{23.2}$$

II. If $z \neq 0$ then

$$A_r(z) \cdot B_{r+1}(z) \neq B_r(z) A_{r+1}(z). \tag{23.3}$$

Consider the inequality (20.2). We cannot have

$$A x^n - B y^n = 0$$

for then $\sqrt[n]{\left|\frac{A}{B}\right|^2}$ would be a rational number of $K(1)$ which is a contradiction. So we can suppose that $|A x^n| > |B y^n|$. As a special value of z we shall then choose

$$z = 1 - \left(\frac{y}{x}\right)^n \frac{B}{A}. \tag{23.4}$$

Hence

$$\sqrt[n]{1-z} = \sqrt[n]{\left(\frac{y}{x}\right)^n \frac{B}{A}}$$

and the root is defined above. It follows by (20.3) and (20.2) the following lemma:

Lemma 1: The inequality $|A x^n| > M^{1/s}$ is true.

Proof: We have

$$2|A x^n| = |A x^n| + |B y^n| + |A x^n| - |B y^n| > |A x^n| + |B y^n| \geqq$$
$$\geqq |A| + |B| \geqq 2 M^{1/s}. \quad (23.5)$$

From this lemma and (20.2) it follows

$$|z| \leqq \left|\frac{C}{A x^n}\right| < \frac{1}{2}, \quad |1-z| = |w| = \left|\frac{B y^n}{A x^n}\right| < 1. \quad (23.6)$$

With this choice of z we now prove the following theorem:

III. For $|z| < \frac{1}{2}$ and $|1-z| < 1$ the following inequalities

$$|A_r(z)| < 1 \quad (23.7)$$

$$|C_r(z)| < |z|^{2r+1} A_r(1) \quad (23.8)$$

are valid.

For the special value (23.4) of z, $C_r(z) \neq 0$.

Proof: The polynomial $F(-\nu-r, -r, 1-\nu, 1-z)$ also satisfies the hypergeometrical differential equation for $A_r(z)$. But the function $(1-z)^r B_r(z)$ satisfies the differential equation for $A_r(z)$ too. Thus the polynomial F must be linearly depending on $A_r(z)$, otherwise $\sqrt[n]{1-z}$ would be a rational function. Hence

$$A_r(z) = A_r(1) \cdot F(-\nu-r, -r, 1-\nu, 1-z).$$

As the polynomial $F(-\nu-r, -r, 1-\nu, w)$ has mere positive coefficients (regarded as a polynomial in w) it follows $A_r(1) > 0$ and further $A_r(0) = 1$. Let us write

$$A_r(z) = a_0 + a_1 w + \cdots + a_r w^r$$

with $a_k > 0$ $(k = 0, 1 \ldots r)$ and it follows from (23.6) that

$$|A_r(z)| < \sum_{k=0}^{r} a_k = A_r(0) = 1.$$

The inequality (23.7) thus holds.

Suppose that $C_r(z)$ is zero for the certain value of z defined by (23.4). According to (23.1) we obtain

$$\sqrt[n]{\left|\frac{B}{A}\right|} = \left|\frac{x}{y}\right| \cdot \left|\frac{A_r(z)}{B_r(z)}\right|$$

which is a contradiction, as $\sqrt[n]{\left|\frac{B}{A}\right|^2}$ is no rational number. (One can see easily that $B_r(z) \neq 0$ for such possible z-values as make $C_r(z)$ zero according to (23.1) and (23.3)).

In the development of $F(-\nu+r+1,\ r+1,\ 2r+2,\ z)$ all the coefficients are positive numbers, and

$$|F(-\nu+r+1,\ r+1,\ 2r+2,\ z)| = \left|\sum_{i=0}^{\infty} b_i z^i\right| < \sum_{i=0}^{\infty} b_i \cdot \frac{1}{2^i} < \sum_{i=0}^{\infty} b_i = \frac{C_r(1)}{\varrho_r}$$

according to (23.2). Further by (23.1) we have $A_r(1) = C_r(1)$ and the relation (23.2) implies the wanted inequality (23.8).

We introduce the following quantities

$$s_r = \binom{2r}{r} q_r n^r, \qquad t_r = q_r n^r \prod_{i=1}^{r} \left(1 - \frac{1}{i\,n}\right)$$

$$s_r A_r(z) = G_r(z) \qquad s_r B_r(z) = H_r(z)$$

where q_r is the product of all the primes of n which divide $r!$, multiple primes being repeated.

The polynomials

$$G_r(z) = q_r n^r \sum_{m=0}^{r} \binom{r+\nu}{m} \binom{2r-m}{r} (-z)^m \tag{23.10}$$

$$H_r(z) = q_r n^r \sum_{m=0}^{r} \binom{r-\nu}{m} \binom{2r-m}{r} (-z)^m \tag{23.11}$$

have coeffecients which are rational integers. (Proved in Siegel's paper.)

In the same way as in Siegel's paper the following relations are derived

$$G_r(z) \cdot H_{r+1}(z) \neq H_r(z) \cdot G_{r+1}(z) \qquad z \neq 0 \tag{23.12}$$

$$|G_r(z)| < s_r \tag{23.13}$$

$$|G_r(z) - (1-z)^{\nu} H_r(z)| < t_r |z|^{2r+1}. \tag{23.14}$$

Moreover the inequality

$$n \cdot s_{r+2} \left(\frac{t_r}{1 - \frac{1}{n}} \right)^{n-1} < \lambda_n^{r+1} \tag{23.15}$$

with $\lambda_3 = 4 \cdot 3^{\frac{9}{2}}$, $\lambda_4 = 4^7$ is true.

§ 4. Two lemmata

24. Suppose that the inequality (20.2) has two solutions (x, y) and (x_1, y_1). Let us also suppose that $L_1 = |A x^n| > |B y^n|$ and further that

$$|A x_1^n| + |B y_1^n| \geqslant |A x^n| + |B y^n|. \tag{24.1}$$

Putting $L_2 = |A x_1^n|$ we shall establish the following lemma:

Lemma 2: The inequality

$$L_2 > M \cdot |2C|^{-n} L_1^{n-1} \tag{24.2}$$

is true.

Proof: In the fields $K(\sqrt{-1})$ and $K(\sqrt{-3})$ the fundamental theorem of number theory is valid, and from the relation $x_1 y = \varepsilon \cdot x y_1$ where ε is an arbitrary unit of the field, it follows either $x = \varepsilon_1 x_1$, $y = \varepsilon_2 y_1$ or $x = \varepsilon_1 y$, $x_1 = \varepsilon_2 y_1$. If $m = 1$ it is immediately clear that we obtain $x = x_1$ and $y = y_1$ in both the cases according to (21.1). If $m = 3$ it follows in the first case that $x = x_1$ and $y = \varepsilon_2 y_1$ according to (22.1). By the fact that (x, y) and (x_1, y_1) are solutions of (20.2) it follows $\varepsilon_2 = 1$, ϱ or ϱ^2 and consequently $y = y_1$ by (22.1). In the second case x, x_1, y and y_1 are units and thus $x = x_1 = 1$, y and $y_1 = 1$ or $-\varrho$. But if $(1, 1)$ is a solution of (20.2) then $(1, -\varrho)$ is not, and vice versa. Thus it follows again $x = x_1$, $y = y_1$ and consequently $x_1 y \neq \varepsilon x y_1$.

Introducing $h = A x^n - B y^n$ it follows $|h| \leqslant |C|$ and $\left| \frac{h}{A x^n} \right| < \frac{1}{2}$. We have

$$\sqrt[n]{\frac{B}{A} \left(\frac{y}{x} \right)^n} = \sqrt[n]{1 - \frac{h}{A x^n}} = 1 - \frac{h}{n A x^n} - \cdots$$

where the n:th root is defined in the former paragraph. It follows

$$\left| 1 - \sqrt[n]{\frac{B}{A} \left(\frac{y}{x} \right)^n} \right| < \frac{|C|}{L_1}. \tag{24.3}$$

If $|Ax_1^n| > |By_1^n|$ we evidently have $\left|\frac{C}{Ax_1^n}\right| < \frac{1}{2}$ by Lemma 1. But this inequality is valid as well if $|By_1^n| > |Ax_1^n|$ for according to the same lemma, (20.2) and (20.3) we obtain

$$|Ax_1^n| \geqslant |By_1^n| - |C| > M^{1/3} - |C| > 2 \cdot |C|.$$

Thus we have

$$\left|1 - \sqrt[n]{\frac{B}{A}\left(\frac{y_1}{x_1}\right)^n}\right| < \frac{|C|}{L_2} \tag{24.4}$$

and the n:th root is defined as the root above.

From (24.3) and (24.4) we obtain

$$\sqrt[n]{\left|\frac{B}{A}\right|}\left|\frac{y}{x} - \varepsilon\frac{y_1}{x_1}\right| < \frac{|C|}{L_1} + \frac{|C|}{L_2}.$$

But as we cannot have $|x_1 y - \varepsilon \cdot x y_1| = 0$ it follows

$$\left|\frac{1}{x x_1}\right| < \sqrt[n]{\left|\frac{A}{B}\right|} \max\left(\frac{2|C|}{L_1}, \frac{2|C|}{L_2}\right)$$

for x, y, x_1 and y_1 are integers of the field. If $L_2 \geqslant L_1$ then the inequality (24.2) is true. If $L_2 < L_1$ we obtain

$$L_2^{1-\frac{1}{n}} < 2|C| \cdot M^{-\frac{1}{n}} L_1^{\frac{1}{n}}$$

and according to (23.5) it follows the contradiction

$$0 \geqslant \tfrac{1}{2}\left(|Ax^n| + |By^n| - |Ax_1^n| - |By_1^n|\right) \geqslant |Ax^n| - |Ax_1^n| - |C| >$$

$$> L_1^{\frac{1}{n-1}}\left\{L_1^{n-1} - \left(\frac{2|C|}{M^{1/n}}\right)^{\frac{n}{n-1}}\right\} - |C| > M^{1/3} - \left(\frac{2|C|}{M^{1/n}}\right)^{\frac{n}{n-1}} - |C| >$$

$$> |C| + 1 - 1 - |C| = 0.$$

Consequently Lemma 2 is proved.

25. **Lemma 3:** There is a positive integer q such that

$$s_q L_1^q \leqslant \frac{M^{1/n}}{n|C|} L_1^{-\frac{1}{n}} L_2^{1-\frac{1}{n}} < s_{q+1} L_1^{q+1}$$

and $q \geqslant 2$ for $n = 4$.

The proof is analogous to that of Siegel.

§ 5. Proof in the case $n=4$

26. With our definition of the roots in the former paragraph we can write

$$\sqrt[n]{\frac{B}{A}\left(\frac{y}{x}\right)^n}=\varepsilon_1\sqrt[n]{\frac{B}{A}}\frac{y}{x},\quad \sqrt[n]{\frac{B}{A}\left(\frac{y_1}{x_1}\right)^n}=\varepsilon_2\sqrt[n]{\frac{B}{A}}\frac{y_1}{x_1}$$

choosing the principal value of $\sqrt[n]{\frac{B}{A}}$ and $\varepsilon_1, \varepsilon_2$ are n:th roots of unity i.e. are units of the regarded field. Introduce $\varepsilon_0=\varepsilon_1\cdot\varepsilon_2^{-1}$.

Consider the value of z defined in (23.4) and let us choose a positive integer $r=q-1$ or $r=q$ (q is the natural number defined in Lemma 3) such that

$$\frac{y_1}{x_1}G_r(z)-\varepsilon_0\frac{y}{x}H_r(z)\neq 0 \tag{26.1}$$

which is possible according to (23.12). The case $n=3$, $q=1$ is treated specially in the next paragraph and we can suppose that $r\geqslant 1$.

According to (23.13), (23.14) and (24.4) we obtain

$$0<\left|G_r(z)-\sqrt[n]{\frac{B}{A}\left(\frac{y}{x}\right)^n}H_r(z)\right|<t_r\left(\frac{|C|}{L_1}\right)^{2r+1}$$

$$\left|G_r(z)-\sqrt[n]{\frac{B}{A}\left(\frac{y_1}{x_1}\right)^n}G_r(z)\right|<s_r\frac{|C|}{L_2}.$$

With the definitions of the n:th roots mentioned above it follows

$$\left|\frac{y_1}{x_1}G_r(z)-\varepsilon_0\frac{y}{x}H_r(z)\right|<\left|\sqrt[n]{\frac{A}{B}}\right|\cdot\left\{s_r\frac{|C|}{L_2}+t_r\left(\frac{|C|}{L_1}\right)^{2r+1}\right\}.$$

By (26.1) the left-hand member is >0 and multiplied by $|(Ax^n)^r x x_1|$ it becomes the absolute value of an integer in $K(\sqrt{-m})$ i.e. it is $\geqslant 1$. Hence

$$1<\frac{1}{M^{1/n}}(L_1\cdot L_2)^{\frac{1}{n}}L_1^r\left\{s_r\frac{|C|}{L_2}+t_r\left(\frac{|C|}{L_1}\right)^{2r+1}\right\}.$$

That this inequality is a contradiction is seen analogously to the corresponding proof in Siegel's paper.

§ 6. Proof in the case $n=3,\ q=1$

27. The case $n=3,\ q=1$ and

$$\frac{y_1}{x_1} G_1(z) = \varepsilon_0 \frac{y}{x} H_1(z) \tag{27.1}$$

is left. The polynomials $A_1(z)$ and $B_1(z)$ have the values

$$A_1(z) = 1 - \tfrac{2}{3} z \qquad B_1(z) = 1 - \tfrac{1}{3} z$$

for $n=3$. According to the definition of ε_0 we have $\varepsilon_0 = 1$, ϱ or ϱ^2.

Putting

$$A x^3 - B y^3 = h, \qquad A x^3 = s'$$

we obtain $|s'| = L_1$ and $z = \dfrac{h}{s'}$. From (27.1) it follows

$$\frac{x_1}{y_1} = \varepsilon_0 \frac{x(3s' - 2h)}{y(3s' - h)}.$$

Hence

$$\frac{A x_1^3 - B y_1^3}{B y_1^3} = \frac{A x^3 (3s' - 2h)^3 - B y^3 (3s' - h)^3}{B y^3 (3s' - h)^3} = \frac{h^3 (2s' - h)}{B y^3 (3s' - h)^3}.$$

Put $(A x_1^3,\ B y_1^3) = d_1$ and it is evidently that $|d_1| \leqslant |C|$. There is an integer d_2 such that

$$\begin{aligned} (A x_1^3 - B y_1^3)\, d_2 &= h^3 (2s' - h)\, d_1 \\ B y_1^3 \cdot d_2 &= B y^3 (3s' - h)^3 d_1. \end{aligned} \tag{27.2}$$

Let us introduce $(2s' - h,\ 3s' - h) = u$, $(2s' - h,\ B y^3) = v$ and it follows that d_2 is a divisor of $h^3 \cdot u v d_1$. However it is easily seen that $|u| \leqslant |h|$ and $|v| \leqslant |h|$ and consequently $|d_2| \leqslant |h^5 C|$. According to (20.2) and (27.2) we obtain

$$|C| \cdot |d_2| \geqslant |h|^3 (2|s'| - |h|)$$

and by (23.5) it follows

$$|C|^4 \geqslant M^{1/2}$$

which is a contradiction according to (20.3).

Consequently the proof of Theorem D is complete.

Chapter III

ON A HYPOTHESIS BY TARTAKOWSKY

§ 1. Introduction

28. In this chapter we shall establish the following theorem:

Theorem E. Let n be a natural number $\geqslant 3$ and M a positive integer which is not a perfect square. If the Diophantine equation

$$x^{2n} - My^{2n} = 1 \tag{28.1}$$

has the solution $x = x_1$, $y = y_1$ in positive integers, then the number $x_1^n + y_1^n \sqrt{M}$ is the fundamental unit ε of the ring $R(\sqrt{M})$ or its square, the latter only occurring in a finite number of cases. If $N(\varepsilon) = -1$ the equation has no solutions with $y \neq 0$.

Since it is always possible to determine the fundamental unit (see § 2) we can decide if the equation (28.1) is solvable and determine the possible solution for every M.

§ 2. On Pell's equation

29. Let M be a positive integer which is not a perfect square and consider the Diophantine equation

$$u^2 - Mv^2 = 1. \tag{29.1}$$

This equation has infinitely many solutions in positive integers u, v. If u and v are natural numbers which satisfy (29.1) we call $u + v\sqrt{M}$ a solution of (29.1). The minimal positive solution of (29.1) we denote by $u_1 + v_1\sqrt{M}$ and we call $u_1 + v_1\sqrt{M}$ the fundamental solution of (29.1). Every solution $u_n + v_n\sqrt{M}$ is obtained by the formula

$$u_n + v_n\sqrt{M} = (u_1 + v_1\sqrt{M})^n$$

where n runs through all the natural numbers and where

$$\left.\begin{aligned} u_n &= u_1^n + \sum_{i=1} \binom{n}{2i} u_1^{n-2i} v_1^{2i} M^i \\ v_n &= \sum_{i=1} \binom{n}{2i-1} u^{n-2i+1} M^{i-1} \end{aligned}\right\} n = 1, 2, 3, \ldots.$$

The fundamental solution can always be determined e.g. by means of the expansion of $\sqrt{M}$ into a simple continued fraction.

Remark: For the proofs see e.g. [11].

§ 3. On the units of $R\sqrt{M}$

30. Suppose that q is a prime $\geqslant 3$ and that M is a positive integer which is not a perfect square. Let q divide n and consider the Diophantine equation

$$x^{2q} - M y^{2q} = 1. \tag{30.1}$$

We denote by $\varepsilon_1 = u_1 + v_1\sqrt{M}$ the fundamental solution of

$$u^2 - M v^2 = 1$$

and by ε an arbitrary solution of this equation with $u, v > 0$. Both ε_1 and ε are units of the ring $R(\sqrt{M})$ with the norm $= +1$, $\varepsilon_1 = \varepsilon_0$ or ε_0^2 where ε_0 is the fundamental unit of the ring $R(\sqrt{M})$. According to § 2 we have the connection

$$\varepsilon = \varepsilon_1^m \tag{30.2}$$

where $m = 1, 2, \ldots$. Our problem is thus reduced to determine the exponent m such that the coefficients of the unit become powers of q. (We call the integers a and b the coefficients of the unit $\varepsilon = a\sqrt{M} + b$). We have to prove that $m = 1$ or 2 are the only possibilities.

The proof is furnished in two stages—at first we show that m cannot be divisible by an odd prime p and afterwards that 4 does not divide m.

31. Suppose that p is an odd prime which divides m. From (30.2) it follows

$$\varepsilon_1^{\frac{m}{p}} = a\sqrt{M} + b$$

where a, b are natural numbers with $(a, b) = 1$.

Hence on one hand we obtain

$$\varepsilon = (a\sqrt{M} + b)^p$$

and on the other hand

$$\varepsilon = y^q\sqrt{M} + x^q.$$

Consequently

$$(a\sqrt{M} + b)^p = y^q\sqrt{M} + x^q. \tag{31.1}$$

Introduce $a = c \cdot k^q$ where c does not contain the q:th power of a prime and $\sqrt{D} = k^q\sqrt{M}$. $\sqrt{D}$ is evidently an irrational number and we obtain

$$(c\sqrt{D} + b)^p = \left(\frac{y}{k}\right)^q\sqrt{D} + x^q. \tag{31.2}$$

As the right-hand member is a number of the ring $R(\sqrt{D})$, k must divide y. Putting $y = k \cdot s$ in (31.2):

$$s^q = c\left[p\,b^{p-1} + \binom{p}{3} c^2 b^{p-3} D + \cdots + c^{p-1} D^{\frac{p-1}{2}}\right].$$

By the definition of c, s^{q-1} is divisible by c. Introducing $s^{q-1} = c \cdot t$ and raising each side of this equation to the q:th power, we obtain

$$t^q = \frac{p^{q-1}\, b^{(q-1)(p-1)}}{c} + H$$

where H is a positive integer. As $(b, c) = 1$, c must divide p^{q-1}. Suppose that $c = p^\alpha$ with $1 \leqslant \alpha \leqslant q-2$. The number H is then divisible by p^{q-1} and the left-hand member is divisible by p^q. But the first term in the right-hand member is only divisible by $p^{q-1-\alpha}$, which is a contradiction. Consequently we must have $\alpha = 0$ or $\alpha = q-1$.

32. In the same way we introduce $b = d \cdot f^q$ where f^q is the highest power of q that divides b. By (31.2) we obtain

$$x^q = p\,c^{p-1} D^{\frac{p-1}{2}} d\,f^q + \cdots + (d\,f^q)^q.$$

The number d is a divisor of the integer $u^{q-1} = \left(\frac{x}{f}\right)^{q-1}$ and we introduce $u^{q-1} = d \cdot v$. We obtain

$$d\,v^q = [p\,c^{p-1} D^{\frac{p-1}{2}} + \cdots]^{q-1}.$$

Since $a\sqrt{M}+b$ is a unit, $(M,b)=1$ and analogously to the argumentation above we see that $d=p^\beta$ with $\beta=0$ or $p-1$.

Thus we obtain the following three possibilities for ε:

$$1^\circ:\varepsilon=(p^{q-1}\sqrt{D}+f^q)^p$$

$$2^\circ:\varepsilon=(\sqrt{D}+f^q)^p$$

$$3^\circ:\varepsilon=(\sqrt{D}+p^{q-1}f^q)^p.$$

In the next three paragraphs we shall demonstrate that these units cannot have coefficients which are powers of q.

§ 4. The case $(p^{q-1}\sqrt{D}+f^q)^p$

33. We have

$$(p^{q-1}\sqrt{D}+f^q)^p=y^q\sqrt{D}+x^q \tag{33.1}$$

(not the same x and y as in § 3). Introducing

$$(p^{q-1}\sqrt{D}+f^q)^{\frac{p-1}{2}}=g\sqrt{D}+h \tag{33.2}$$

we have

$$y^q\sqrt{D}+x^q=(g\sqrt{D}+h)^2\,(p^{q-1}\sqrt{D}+f^q)$$

and consequently

$$y^q=g^2Dp^{q-1}+2ghf^q+h^2p^{q-1} \tag{33.3}$$

$$x^q=g^2Df^q+2ghDp^{q-1}+h^2f^q. \tag{33.4}$$

From (33.2) we see that $g\equiv 0 \pmod{p^{q-1}}$ and consequently $y\equiv 0 \pmod{p}$. Put $g=g_1\cdot p^{q-1}$, $y=py_1$ and from (33.3) we obtain

$$py_1^q=g_1^2p^{2q-2}D+2h\cdot g_1f^q+h^2$$

But according to (33.1) we have

$$f^{2q}-p^{2q-2}D=1. \tag{33.5}$$

Hence

$$py_1^q=[g_1(f^q+1)+h]\cdot[g_1(f^q-1)+h]. \tag{33.6}$$

The two factors of the right-hand member are relatively prime, for it appears from the relation

$$h^2-g_1^2Dp^{2q-2}=h^2-(f^{2q}-1)g_1^2=1$$

that y is odd.

We distinguish between two cases: Either we have $f^q - 1 \equiv 0 \pmod{p^{2q-2}}$ and $g_1(f^q+1)+h \equiv 0 \pmod{p}$ or $f^q+1 \equiv 0 \pmod{p^{2q-2}}$ and $g_1(f^q-1)+h \equiv 0 \pmod{p}$. It is sufficient to treat the first case since the second case can be treated in a similar way.

We obtain from (33.6)

$$g_1(f^q+1)+h = p\xi^q, \quad g_1(f^q-1)+h = \eta^q \tag{33.7}$$

where ξ and η are positive integers. Hence

$$g = \frac{p^{q-1}}{2}(p\xi^q - \eta^q), \quad h = \tfrac{1}{2}[(f^q+1)\eta^q - (f^q-1)p\xi^q].$$

Introducing these values in (33.4) it is easily deduced

$$2x^q = (f^q-1)p^2\xi^{2q} + (f^q+1)\eta^{2q}.$$

Further we have

$$2N(g\sqrt{D}+h) = 2 = (f^q+1)\eta^{2q} - (f^q-1)p^2\xi^{2q}.$$

According to the last two equations we obtain at last

$$x^q - (f^q+1)\eta^{2q} = -1.$$

As $f \neq 2$ this equation has at most one solution except possibly in the case $f=1$, and $f=1$ is impossible according to (33.5). Thus $x=f$, $\eta=1$ is the only solution. By (33.7) we see however that $\eta > 1$.

Thus we have shown that $(p^{q-1}\sqrt{D}+f^q)^p$ cannot have coefficients, which are powers of q.

§ 5. The case $(\sqrt{D}+f^q)^p$

34. From

$$(k^q\sqrt{M}+f^q)^p = y^q\sqrt{M}+x^q \tag{34.1}$$

we obtain

$$f^{2q} - Mk^{2q} = x^{2q} - My^{2q} = 1$$

since the norm of a unit is 1. But the Diophantine equation

$$\xi^{2q} - M\eta^{2q} = 1$$

has at most one solution if $M > 2$ and no solution if $M = 2$. Thus we get $f=x$, $k=y$ and by (34.1) it follows $p=1$ which is a contradiction.

§ 6. The case $(\sqrt{D}+p^{q-1}f^q)^p$

35. We have

$$\varepsilon=(\sqrt{D}+p^{q-1}f^q)^p=y^q\sqrt{D}+x^q.$$

Introducing

$$(\sqrt{D}+p^{q-1}f^q)^{\frac{p-1}{2}}=g\sqrt{D}+h$$

it follows

$$(g\sqrt{D}+h)^2(\sqrt{D}+p^{q-1}f^q)=y^q\sqrt{D}+x^q$$

and consequently

$$y^q=g^2D+2ghp^{q-1}f^q+h^2$$
$$x^q=g^2Dp^{q-1}f^q+2ghD+h^2p^{q-1}f^q.$$

Since we have

$$D=p^{2q-2}f^{2q}-1$$

it follows

$$y^q=g^2(p^{2q-2}f^{2q}-1)+2ghp^{q-1}f^q+h^2=[g(p^{q-1}f^q+1)+h]\cdot$$
$$\cdot[g(p^{q-1}f^q-1)+h].$$

The two factors of the right-hand member are relatively prime, for according to

$$h^2-g^2D=1 \tag{35.1}$$

it is obvious that y is odd. Thus we obtain

$$g(p^{q-1}f^q+1)+h=v^q$$
$$g(p^{q-1}f^q-1)+h=u^q$$

with $u\cdot v=y$. Hence

$$g=\tfrac{1}{2}(v^q-u^q),\quad h=\tfrac{1}{2}[u^q(f^qp^{q-1}+1)-v^q(f^qp^{q-1}-1)]$$

and according to (35.1) we obtain

$$2=(p^{q-1}f^q+1)u^{2q}-(p^{q-1}f^q-1)v^{2q}. \tag{35.2}$$

However using a result due to Siegel (Theorem I, p. 5) about the Diophantine equation $Ax^n-By^n=C$ there are no solutions in positive integers of (35.2) except $u=v=1$ if the inequality

$$(p^{2q-2}f^{2q}-1)^{q-1}\geqslant 2^{8q}\cdot q^{\frac{2q^2}{q-1}}$$

holds. It is easily seen that the inequality is valid if $f\geqslant 5$, p, $q\geqslant 3$ and if $f\geqslant 4$, p or $q\geqslant 5$. If $f\geqslant 2$, $q\geqslant 5$ it is true too, and also if $f=1$, p, $q\geqslant 5$. The remaining cases are

f	p	q
4	3	3
3	5	3
3	3	3
2	5	3
2	3	3
1	5	3
1	3	5
1	3	3

1) For $f=4$, $p=q=3$ we obtain

$$(\sqrt{D}+576)^3=y^3\sqrt{D}+x^3$$

and from the fact that the norm is 1 we obtain the two equations

$$576^2-D=1$$

$$D+3\cdot 576^2=y^3$$

and consequently $y^3=1327103$ which is impossible as y is an integer.

The corresponding equations in the other cases are

2) $(\sqrt{D}+675)^5=y^3\sqrt{D}+x^3$ and $y^3=3321500782501$

3) $(\sqrt{D}+243)^3=y^3\sqrt{D}+x^3$ and $y^3=236195$

4) $(\sqrt{D}+200)^5=y^3\sqrt{D}+x^3$ and $y^3=25599520001$

5) $(\sqrt{D}+72)^3=y^3\sqrt{D}+x^3$ and $y^3=20735$

6) $(\sqrt{D}+25)^5=y^3\sqrt{D}+x^3$ and $y^3=6242501$

7) $(\sqrt{D}+81)^3=y^5\sqrt{D}+x^5$ and $y^5=26243$

8) $(\sqrt{D}+9)^3=y^3\sqrt{D}+x^3$ and $y^3=323$.

All these values of y are no integers however.

So far we have proved that the number m (defined in § 2) cannot be divisible by an odd prime number, but must be 1 or a power of 2.

§ 7. Proof that m is 1 or 2

36. Let ε be an arbitrary unit of $R(\sqrt{M})$ with $N(\varepsilon)=+1$ and suppose that the fourth power of the unit has coefficients which are q:th powers.

$$\varepsilon = a\sqrt{M} + b \tag{36.1}$$

$$\varepsilon^4 = y^q\sqrt{M} + x^q. \tag{36.2}$$

Introducing

$$\varepsilon^2 = k\sqrt{M} + l \tag{36.3}$$

we obtain

$$a^2 M + b^2 + 2ab\sqrt{M} = k\sqrt{M} + l \tag{36.4}$$

$$k^2 M + l^2 + 2kl\sqrt{M} = y^q\sqrt{M} + x^q. \tag{36.5}$$

Consequently k is even and since $(a, b) = (k, l) = 1$ we have $k = 2^{q-1}s^q$, $l = t^q$ with $2s \cdot t = y$. We distinguish between two cases:

$$1^\circ.\ a = 2^{q-2}u^q,\ b = v^q.$$

With respect to (36.1) and (36.4) it follows

$$2v^{2q} - 1 = t^q \tag{36.6}$$

and from (36.3) and (36.5)

$$2t^{2q} - 1 = x^q.$$

But the Diophantine equation

$$x^q - 2y^{2q} = -1$$

has at most one solution in positive integers except $x = y = 1$. If $v = t = 1$ we obtain $x = 1$ which is a contradiction by (36.2). Thus we must have $v = t$ and $t = x$ i.e. again $x = 1$ which is impossible.

Remark: If M is even, 1° is the only possibility as $(b, M) = 1$, and we have proved what was purposed. This fact is not used in the following discussions.

37. $2^\circ.\ a = u^q,\ b = 2^{q-2}v^q.$

According to (36.1) (36.4) resp. (36.3) and (36.5) we obtain the following two Diophantine equations

$$2^{2q-3}v^{2q} - t^q = 1 \tag{37.1}$$

$$2t^{2q} - x^q = 1. \tag{37.2}$$

We shall prove that these two equations cannot both have solutions in positive integers (v, t) resp. (t, x). (The solution $t = x = 1$ is evidently of no interest.)

Putting $z_1 = 2^{2q-3}v^{2q}$, $z_2 = x^q$ it follows

$$1-\frac{t^q}{2^{2q-3}v^{2q}}=\frac{1}{z_1}$$

and consequently

$$\frac{t\sqrt[q]{8}}{4v^2}=\sqrt[q]{1-\frac{1}{z_1}}>1-\frac{1}{z_1}.$$

Hence

$$0<1-\frac{t\sqrt[q]{8}}{4v^2}<\frac{1}{z_1}. \tag{37.3}$$

In the same way we obtain by (37.2)

$$\frac{2t^{2q}}{x^q}=\frac{1}{x^q}+1$$

and

$$\frac{8t^{6q}}{x^{3q}}=\left(\frac{1}{x^q}+1\right)^3=\frac{1}{x^{3q}}+\frac{3}{x^{2q}}+\frac{3}{x^q}+1<\frac{4}{z_2}+1$$

for $x>1$. Hence

$$\frac{\sqrt[q]{8}t^6}{x^3}<\sqrt[q]{1+\frac{4}{z_2}}<1+\frac{4}{z_2}$$

and at last

$$0<\frac{\sqrt[q]{8}t^6}{x^3}-1<\frac{4}{z_2}. \tag{37.4}$$

According to (37.3) and (37.4) we obtain

$$\sqrt[q]{8}\left|\frac{t}{4v^2}-\frac{t^6}{x^3}\right|<\frac{1}{z_1}+\frac{4}{z_2}<\frac{2}{z_1}$$

as $z_2>4z_1$, by (37.1) and (37.2). Further $|x^3-4v^2t^5|\neq 0$ as x is odd. Hence

$$\frac{t\sqrt[q]{8}}{4v^2x^3}<\frac{2}{z_1}$$

and according to (37.1) and (37.2) we obtain the inequality

$$8t^q(t^q+1)^q<8^q(2t^{2q}-1)^3\frac{t^q+1}{2^{2q-3}}$$

or

$$t^q(t^q+1)^{q-1}<2^q(2t^{2q}-1)^3.$$

Now t is odd, i.e. $t\geqslant 3$. However this inequality is impossible for $q\geqslant 7$.

38. Let $q=5$. The relation (37.3) can be exchanged for

$$0<1-\frac{t}{\sqrt[5]{4}\cdot 2v^2}<\frac{1}{2z_1} \tag{38.1}$$

as $(1-z_1^{-1})^{\frac{1}{5}}>1-(2z_1)^{-1}$ if $z_1\geqslant 2$. From (37.2) we obtain

$$\frac{x^5}{2t^{10}}=1-\frac{1}{z_3}$$

with $z_3=2t^{2q}$. In the same way as above the inequality

$$\frac{x^2}{\sqrt[5]{4}\,t^4}>1-\frac{2}{z_3} \tag{38.2}$$

is valid. (38.1) and (38.2) give

$$\frac{1}{\sqrt[5]{4}}\left|\frac{x^2}{t^4}-\frac{t}{2v^2}\right|<\frac{1}{2z_1}+\frac{2}{z_3}<\frac{1}{z_1}$$

as $z_3>4z_1$. The number t is odd and consequently $|2x^2v^2-t^5|\geqslant 1$. Thus we obtain

$$(t^5+1)^5<t^{20}(t^5+1)$$

which is a contradiction. Herewith we have proved that the two Diophantine equations cannot both be solved in integers (v, t) resp. (t, x).

Remark: For $q=5$ it is not necessary to establish the proof above. The fact is that Skolem [17] has proved that the Diophantine equation $2x^5-y^5=1$ has no solutions in positive integers except $x=y=1$.

For $q=3$ we know that the only solution in integers of $2x^3-y^3=1$ is $x=y=1$. (See [13]).

Thus we have proved that the fourth power of a unit ε with $N(\varepsilon)=+1$ cannot have coefficients which are q:th powers.

39. Let us finally treat the case $N(\varepsilon)=-1$ where ε is an arbitrary unit of the field $R(\sqrt{M})$.

Suppose that

$$\varepsilon=a\sqrt{M}+b$$

$$\varepsilon^2=y^q\sqrt{M}+x^q.$$

Hence $2ab=y^q$ and since $N(\varepsilon)=-1$ it follows

$$2b^2+1=x^q.$$

But this Diophantine equation has only the solution $b=11$, $x=3$ and $q=5$ and this value of b does not satisfy the relation $2ab=y^q$ above. This result follows from a theorem due to Nagell [10]: Let n be an odd integer $\geqslant 3$ and let A be a square-free integer $\geqslant 1$. If the class number of the field $K(\sqrt{-A})$ is not divisible by n, the Diophantine equation $Ax^2+1=y^n$ has no solutions in integers x and y for y odd and $\geqslant 1$, apart from $x=\pm 11$, $y=3$ for $A=2$ and $n=5$.

If ε^4 has coefficients which are q:th powers we obtain

$$\varepsilon^2 = k\sqrt{M}+l$$

$$\varepsilon^4 = y^q\sqrt{M}+x^q$$

and since k is even, we must have $l=l_1^q$ and thus again

$$2b^2+1=l_1^q$$

which is impossible. Thus there are no solutions of (28.1) if $N(\varepsilon_1)=-1$ where ε_1 is the fundamental unit of $R(\sqrt{M})$.

Consider the case when we have a solution given by the square of the fundamental unit of $R(\sqrt{M})$.

$$\varepsilon = a\sqrt{M}+b$$

$$\varepsilon^2 = y^q\sqrt{M}+x^q.$$

We can easily see that we obtain either

$$2v^{2q}-1=x^q$$

or

$$2^{2q-1}v^{2q}-1=x^q$$

with $b=v^q$ resp. $b=2^{q-1}v^q$. Since there is at most one solution (except $x=v=1$ which is of no interest) of every equation there are only a finite number of M such that the square of the fundamental unit of $R(\sqrt{M})$ has coefficients which are q:th powers.

Thus we have furnished a complete proof of the theorem formulated at the beginning of this chapter.

[1] B. Delaunay, Vollständige Lösung der unbestimmten Gleichung $X^3 q + Y^3 = 1$ in ganzen Zahlen. Math. Zeitschr. Bd 28 (1928), S. 1–9.

[2] Y. Domar, On the Diophantine equation $|A x^n - B y^n| = 1$, $n \geqslant 5$. Math. Scand. 2 (1954), p. 29–32.

[3] L. Fjellstedt, On a class of Diophantine equations of the second degree in imaginary quadratic fields. Arkiv f. Matematik bd 2 (1953), p. 435–461.

[4] P. Häggmark, On a class of quintic Diophantine equations in two unknowns. Dissertation, Uppsala (1952).

[5] K. Knopp, Elemente der Funktionentheorie. Sammlung Göschen bd 1109, Berlin (1955), S. 132–141.

[6] W. Ljunggren, A Diophantine equation with two unknowns. Den 10. Skandinaviske Matematikerkongres 1946, s. 265–270.

[7] ——, Einige Eigenschaften der Einheiten reeller quadratischer und reinbiquadratischer Zahlkörper. Oslo (1937). Skrifter utgitt av det Norske Videnskabs-Akademi i Oslo. I. Mat.-Naturv. Klasse, no 12 (1936).

[8] ——, Solutions complète de quelques équations du sixième degré à deux indeterminées. Arch. Math. Naturvid. 48, no 7 (1946), p. 177–211.

[9] ——, On an improvement of a theorem by T. Nagell concerning the Diophantine equation $A x^3 + B y^3 = C$. Math. Scand. 1 (1953), p. 297–309.

[10] T. Nagell, Contributions to the theory of a category of Diophantine equations of the second degree with two unknowns. Nova acta regiæ societatis scientarum Upsaliensis. Ser. IV, vol. 16, nr 2 (1955).

[11] ——, Introduction to Number Theory. New York & Stockholm 1951, p. 75, 204–208, 235–246.

[12] ——, On a special class of Diophantine equations of the second degree. Arkiv för Matem. Bd 3, nr 2 (1954), p. 51–65.

[13] ——, Solution complète de quelques équations cubique à deux indéterminées. Journ. de Math. t. IV, 9e sér. (1925), p. 209–270.

[14] J. Schäffer, The equation $1^p + 2^p + \cdots + n^p = m^p$. Acta Math. 95 (1956), p. 155–189.

[15] C. L. Siegel, Die Gleichung $a x^n - b y^n = c$. Math. Ann. Bd 114 (1937), S. 57–68.

[16] T. Skolem, Einige Sätze über gewisse Reihenentwicklungen und exponentiale Beziehungen mit Anwendungen auf diophantische Gleichungen. Skrifter utgitt av det Norske Videnskabs-Akademi i Oslo, I. Mat.-Naturv. Klasse, no 6 (1933).

[17] ——, En metode til behandling av ubestimte ligninger. Chr. Michelsens Inst. Beretn. IV, 6, Bergen (1934).

[18] ——, The use of a p-adic method in the theory of Diophantine equations. Bull. de la Soc. Math. de Bélgique, VII. Bruxelles (1954–55), p. 84–92.

[19] W. Tartakowsky, Auflösung der Gleichung $x^4 - \varrho y^4 = 1$. Bull. de l'Académie des Sciences URSS, Bd 20 (1926). S. 301–324.

[20] A. Thue, Über Annäherungswerte algebraischer Zahlen. Journ. für Math. 135 (1909), S. 284–305.

[21] ——, Berechnung aller Lösungen gewisser Gleichungen von der Form $a x^r - b y^r = f$. Videnskabsselskabets Skrifter, I, No 4, Kristiania (1918).